

Table of Contents

1.1	Policy	1
1.2	Reference	1
1.3	Scope.....	1
1.4	Responsibilities.....	1
	A. The Inspector General.....	1
	B. The Deputy Inspector General	1
	C. Assistant Inspectors General.....	1
	D. General Counsel.....	1
	E. The Assistant Inspector General for Management and Planning	1
	F. Master Manual Holders	1
1.5	Manual Structure	1
	A. Volumes.....	1
	B. Number System.....	1
	C. Table of Contents.....	2
1.6	Chapter Content.....	2
	A. Required Sections	2
	B. Optional Sections.....	2
1.7	Procedures.....	3
	A. Publication	3
	B. Preparation.....	3
	C. Coordination	3
	D. Approval	4
	E. Dissemination	4
	F. Circulation and Maintenance.....	4
	G. Revisions and Revalidation	5
	H. Interim Guidance	5
	APPENDIX A.....	7
	APPENDIX B.....	8
	APPENDIX C.....	9

Table of Contents

002.1	Policy.....	1
002.2	Reference.....	1
002.3	Scope.....	1
002.4	Procedures.....	1
002.5	Mission Statement.....	1
002.6	Organizational Structure.....	1
002.7	Function Statements.....	1
	A. Inspector General.....	1
	B. Deputy Inspector General.....	2
	C. Senior Counsel.....	2
	D. General Counsel.....	2
	E. Assistant Inspector General, Audit Division.....	3
	F. Assistant Inspector General, Investigations Division.....	3
	G. Assistant Inspector General, Evaluation and Inspections Division.....	3
	H. Assistant Inspector General, Oversight and Review Division.....	4
	I. Assistant Inspector General, Management and Planning Division.....	4

Table of Contents

003.1	Policy	2
003.2	Reference	2
003.3	Scope.....	2
003.4	Procedures.....	2
003.5	Authorities Retained by the Inspector General.....	2
003.6	Delegation to the Deputy Inspector General	3
003.7	Delegation to the General Counsel	3
003.8	Delegation to the Assistant Inspector General, Audit Division.....	4
003.9	Delegation to the Assistant Inspector General, Investigations Division	4
003.10	Delegation to the Assistant Inspector General, Evaluation and Inspections Division	4
003.11	Delegation to the Assistant Inspector General, Oversight and Review Division	4
003.12	Delegation to the Assistant Inspector General, Management and Planning Division	5
003.13	Delegation to the Contracting Officer	5
003.14	Redelegation of Authority	6
003.15	Continuity of Operations	6

Table of Contents

030.1	Policy	1
030.2	Reference	1
030.3	Scope	1
030.4	Responsibilities	1
	A. Employees	1
	B. Supervisors	1
	C. The Oversight and Review Division	2
	D. The Office of General Counsel	2
	E. The Deputy Inspector General	2
030.5	Procedures	2
	A. Standards of Conduct	2
	B. Outside Employment.....	4
030.6	Reporting Requirements.....	8
	A. Occurrences an Employee Must Report.....	8
	B. Actual or Potential Conflicts of Interest.....	8
APPENDIX A	Request for Permission to Engage in Outside Employment.....	9

Table of Contents

222.1	Policy	1
222.2	Reference	1
222.3	Scope.....	1
222.4	Responsibilities.....	1
	A. The Inspector General.....	1
	B. Security Programs Manager	1
	C. Office Heads	2
	D. Security Officers.....	2
	E. Employees and Contractors	2
222.5	Definitions	2
222.6	Procedures.....	3
	A. Identification and Markings.....	3
	B. Storage and Transmission.....	4
	C. Access and Dissemination	6
	D. Destruction and Reuse	7
	E. SBU Collected and Provided by Other Agencies	9
	F. Incident Reporting and Handling Requirements	9

Table of Contents

001.1	Policy.	1
001.2	Reference.	1
001.3	Scope.....	1
001.4	Procedures.....	1
001.5	Mission Statement.	1
001.6	Mission Responsibilities.....	2
001.7	Law Enforcement Authorities.....	2

032.1	Policy	1
032.2	Reference	1
032.3	Scope.....	1
032.4	Procedures.....	1
032.5	Media Requests That Must Be Referred to or Coordinated With Investigations Division Headquarters	1
	A. News of International/National/Major Regional Interest	2
	B. Requests from National or Significant Media Organizations.....	2
	C. News Conferences	2
	D. Comments on Specific Issues (Legislative Proposals, Budget).....	2
032.6	Media Contacts and Release of Information by Field Office SAC	2
	A. Inquiries Regarding Federal Prosecutions and Litigation	2
	B. Release of Information Regarding Ongoing Investigations	3
	C. Disclosure After Arrest and a Criminal Complaint, Indictment, or Information Has Been Issued.....	3
	D. Release of Criminal History Information	3
	E. Information That Should Not Be Released Regarding Criminal Investigations	4
	F. Release of Information Regarding Civil Litigation	4
	G. Information That Should Not Be Released Regarding Civil Matters.....	4
032.7	Assisting/Deterring News Gathering	5
032.8	Record of Media Coverage	5
032.9	Publications or Speeches by Investigations Division Personnel	5
APPENDIX A.....		7

Table of Contents

100.1	Policy	1
100.2	Reference	1
100.3	Scope.....	1
100.4	Administrative Recordkeeping	1
	A. File Numbering.....	1
	B. Document and Correspondence Numbering.....	1
100.5	Investigative File Retention, Storage and Disposition	1
	A. Complaints Classified as Management Referrals or Informations	1
	B. Complaints Classified as Monitored Referrals (R).....	2
	C. Record Destruction Methods	2
	D. Complaints Classified as Investigations (I).....	3
	E. Exception to Disposition of Complaints Classified as Investigations (I)	4
	F. Investigations of Sexual Abuse in Confinement Settings.....	5
100.6	Time and Attendance.....	5
	A. Basic Hours of Work	5
	B. Bi-weekly Time and Activity Reporting	8
	C. Total Bi-Weekly Hours.....	10
	D. Overtime and Other Pay	10
	E. Law Enforcement Availability Pay (LEAP) Act of 1994.....	10
	F. LEAP Certifications.....	11
100.7	Annual Home-to-Work Use of Official Government Vehicle and Drivers License Certification	12
	A. Certification for Home-to-Work Use of Official Government Vehicle	12
	B. Annual Driver's License Certifications	13
100.8	Official Correspondence.....	13
	A. Memorandum Format	13
	B. Letter Format	13
100.9	Requests for Review of OIG Files.....	13
	A. Law Enforcement.....	13
	B. Background Investigation Requests	14
	C. Giglio/Henthorn Requests from federal prosecutors for information regarding prosecution witnesses	14
	D. Other Special Requests	16
100.10	Congressional Inquiries	17

100.11	Hotline Operations.....	17
100.12	Safety and Seat Belt Usage.....	17
	A. Emergency Equipment.....	17
	B. Seat Belts	17
100.13	Employee Transfers and Mobility Agreements.....	18
	A. Official Time for Relocating	18
	B. Mobility Agreements	18
100.14	Serious Incident Management	19
	A. Notification	19
	B. Definition of a Serious Incident.....	19
100.15	External Reports	19
	A. Annual Reports	20
	B. Semiannual Reports	21
	C. Quarterly Reports.....	21
100.16	Internal Reports	22
	A. Annual Reports	22
	B. Semiannual Reports	22
	C. Quarterly Reports.....	22
	D. Monthly Reports	23
	E. Weekly Reports	24
	F. Miscellaneous Reports.....	24
APPENDIX A. Sample Box Marking and Addressing for Investigative Case Files Sent to Records Storage Facility.....		26
APPENDIX B. Inventory Transmittal (OIG Form III-100/6).....		27
APPENDIX C. LEAP Certifications and Sample Memoranda and Calculation Steps		28
APPENDIX D. Annual OGV Home-to-Work and Driver’s License Certifications		29
APPENDIX E. OIG Special Agent Mobility Agreement (OIG Form III-100/5).....		30
APPENDIX F. Definitions of Terms in the Prison Rape Elimination Act.....		31

Table of Contents

200.1	Policy	1
200.2	Reference	1
200.3	Scope.....	1
200.4	Procedures.....	1
	A. Knowledge.....	1
	B. Abilities.....	1
	C. Skills	2
200.6	Planning, Execution, Reporting, and Information Management	2
	A. Planning	2
	B. Execution	2
	C. Reporting	3
	D. Information Management	3
200.7	Ethics and Standards of Conduct	4
	A. Contact With Represented Persons.....	4
	B. Contact With Complainants, Victims, Witnesses, Informants, or Subjects	4
	C. Contact With Jurors	4
	D. Ethics Training.....	4
200.8	Professionalism.....	4
200.9	Due Professional Care	5
	A. Objectivity and Impartiality.....	5
	B. Thoroughness.....	5
	C. Legal Requirements	5
	D. Appropriate Techniques.....	5
	E. Timeliness.....	5
	F. Complete and Accurate Documentation.....	6
200.10	Testifying in Other Than OIG Matters	6
209.11	Use of Emergency Equipment.....	6
	A. Safety	6
	B. High Speed Pursuit Driving.....	6
	C. Traffic Stops	6
	D. Local Law Enforcement Support.....	6
	E. Approved Equipment.....	7
	F. Reporting Usage	7

Table of Contents

205.1	Policy	1
205.2	Reference.....	1
205.3	Scope.....	1
205.4	Reporting Complaints.....	1
	A. Where to Report Allegations.	1
	B. Information to Report.....	1
	C. Coordination with the Office of Professional Responsibility – DOJ Attorney Misconduct.....	1
	D. Federal Bureau of Investigation Whistleblower Complaints.....	2
205.5	Reporting Complaints – Classes of Complaints	2
	A. Classification No. 1	2
	B. Classification No. 2.....	2
	C. Classification No. 3.....	2
205.6	Processing Complaints.....	3
	A. Responsibility for IDMS Entry	3
	B. IDMS Requirements	3
	C. Deleting IDMS Entries	4
205.7	Disposition of Complaints.	4
	A. Responsibility for Disposition of Complaints.....	4
	B. Disposition Timeframes.....	5
205.8	Disposition of Complaints – Criteria and Procedures.....	5
	A. OIG Investigations – IDMS Classification “I.”	5
	B. Monitored Referrals – IDMS Classification “R.”	6
	C. Management Review – IDMS Classification “M.”	7
	D. Information – IDMS Classification “F.”.....	8
	E. Consolidated – IDMS Classification “C.”	8
	F. Non-DOJ – IDMS Classification “X.”.....	8
205.9	Processing FBI Whistleblower Complaints.....	9
	A. Timeframes	9
	B. Factors.....	10
205.10	Civil Rights Complaints.....	10
	A. Timeframes	10
	B. Patriot Act Complaints.....	10
	C. Complaints Pending CRT Decision	10
	D. Disposition	10

E.	Preliminary Inquiry	10
205.11	Confidentiality of Complainants and Witnesses.....	11
A.	Disclosure Considerations	11
B.	Confidentiality Policy	11
C.	Retaliation Prohibitions	12
D.	Disclosure Requests	12
205.12	Processing Allegations of Sexual Abuse in Confinement Settings	13
A.	Disposition	13
B.	IDMS and iManage.....	13
C.	Inmate-on-Inmate Sexual Abuse.....	14
D.	Confidentiality	14
E.	Acknowledgment Letters	15
APPENDIX A.	Typical Types of Misconduct To Be Reported to the OIG	16
APPENDIX B.	Field Office Form for Dissemination/Referral of Complaints	17
APPENDIX C.	Sample Reveal Letter	18
APPENDIX D.	Definition of Terms in the <i>Prison Rape Elimination Act</i>	19

Table of Contents

207.1	Policy.....	1
207.2	Reference	1
207.3	Scope.....	1
207.4	Opening Investigations	1
	A. Geographic Areas	1
	B. Headquarters Coordination Responsibility.....	1
	C. Investigations Data Management System.....	1
	D. FBI Notification Letters.....	2
207.5	Managing Investigations.....	2
	A. General Principles.....	2
	B. Timeframes for Working and Completing Investigations	3
	C. Investigative Work Plans	4
	D. Operational Plans.....	5
	E. Compliance with the Rehabilitation Act.....	5
207.6	Management Tools and Responsibilities.....	5
	A. Field Office Productivity Chart	5
	B. Quality, Objectivity, Timeliness, and Appropriate Direction of Investigations.....	6
207.7	Office Case File Folder.....	6
	A. Work Folders	6
	B. Document Placement in the Office Case File Folder	7
	C. File Content Summary Sheet and Case Review Record.....	7
	D. Special Contents	7
	E. Disposition of Investigative Notes and Work Papers	8
207.8	Memorandum of Investigation	8
207.9	Report of Investigation	9
	A. Review and Approval	9
	B. Distribution	9
	C. Distribution Exceptions	9
207.10	Abbreviated Report of Investigation	10
	A. Authorization for Use	10
	B. Distribution	11
207.11	Priority Cases.....	12
	A. Types of Priority Cases.....	12

	B.	Investigative Work Agreement.....	12
	C.	Reports of Investigation.....	13
207.12		Interim ROIs	13
	A.	When Required	13
	B.	Distribution.....	14
207.13		Prosecution Reports	14
	A.	When Required	14
	B.	Distribution	15
207.14		Auxiliary Investigations.....	15
	A.	Requests for AUX Investigations	15
	B.	Case Management.....	16
	C.	AUX Report.....	16
	D.	Distribution	16
	E.	Controlling Office Actions When Closing Predicating Case	16
207.15		Fugitive Status	17
	A.	Fugitive	17
	B.	Wanted Person	17
	C.	OIG/Field Office/Agent Responsibility.....	17
	D.	Case Management.....	17
	E.	Documentation.....	18
	F.	Apprehension Investigation Request	18
	G.	Subsequent Information.....	19
	H.	Arrest of the Fugitive	19
	I.	Inactive Status.....	20
	J.	Closing Inactive Fugitive Cases	20
207.16		Sworn Statements	21
	A.	Objectives and Strategy	21
	B.	Authority.....	22
	C.	Non-Criminal Cases.....	22
	D.	Criminal Cases.....	22
	E.	Sworn Statement Formats: Written Affidavit.....	22
	F.	Sworn Statement Formats: Audio or Audio-Video Recorded Affidavit	23
	G.	Recording Custodial Interviews	25
	H.	Copies	25
207.17		Documenting Statements	25
	A.	Documents	25
	B.	Refusal To Be Placed Under Oath.....	25
207.18		Special Procedures Regarding the FBI	26

	A.	Notification to Subjects	26
	B.	Nondisclosure Agreement for Attorneys in FBI Cases	26
207.19		Closing Investigations	26
	A.	Criteria	26
	B.	Sixty-Day Cases.....	27
	C.	Reports.....	28
	D.	iManage	28
	E.	IDMS	29
	F.	Supervisory Approval	29
	G.	Exoneration Letters.....	29
207.20		Procedural Reform Recommendations	29
	A.	Field Office Responsibilities	29
	B.	Distribution.....	29
207.21		Monitored Referral Investigations (IDMS Classification “R”).....	29
	A.	Responsibility	30
	B.	Monitoring Methods	30
	C.	Oversight Responsibility	30
207.22		Initiatives	31
	A.	Definition.....	31
	B.	Opening an Initiative	31
	C.	Administrative Procedures.....	31
207.23		Use of (b) (7)(E) in BOP Investigations.....	32
	A.	OIG (b) (7)(E) Compliance Manager	32
	B.	Authorized Communication Systems	32
	C.	Authorized Users	32
	D.	Deactivation of Users	33
	E.	Authorized Use of (b) (7)(E)	33
	F.	Prohibited Use of (b) (7)(E)	33
	G.	Recordkeeping	33
	H.	Safeguarding (b) (7)(E) Information	33
	I.	Security Incidents	34
207.24		Special Procedures Regarding the Management of Investigations of Allegations of Sexual Abuse in Confinement Settings	34
	A.	Training.....	34
	B.	Standards.....	34
	C.	Victim Safety	34
	D.	Victim Advocates	35
	E.	Use of Polygraph	35
	F.	Refusal of Victim to Cooperate.....	35

G.	Departure of Subject or Victim.....	35
H.	Proving Contact	35
I.	Presentation for Prosecution.....	35
J.	Administrative Investigations.....	35
K.	Processing Non-DOJ PREA Allegations.....	35
207.25	Conflict of Interest Investigations	36
A.	Upon Referral to Prosecutor	36
B.	Disposition of Referral When Case is Closed	36
C.	When Adverse Findings Have Been Made.....	37
APPENDIX A.	Memorandum of Understanding Between the Office of the Inspector General and Federal Bureau of Prisons	
APPENDIX B.	Policy Concerning Electronic Recording of Statements (Deputy Attorney General Memorandum, May 12, 2014)	

Table of Contents

210.1	Policy	1
210.2	Reference	1
210.3	Scope.....	1
210.4	Report Writing Guidelines That Apply to All Investigative Documents	1
	A. Application	1
	B. Content Standards.....	1
	C. Format and Style Standards	2
210.5	Memorandum of Investigation Guidelines	2
	A. Quality Standards.....	2
	B. Personally Identifiable Information.....	2
	C. Separate Activities	3
	D. MOI Preparation Timeframes.....	3
	E. Review and Approval	3
	F. MOI Requirement Exceptions	3
210.6	Report of Investigation Guidelines	3
	A. Concept and General Format	4
	B. Content Standards.....	4
	C. ROI Format and Style Standards	4
210.7	Abbreviated Report of Investigation Guidelines	4
210.8	Procedural Reform Recommendation Guidelines	4
	A. Purpose	5
	B. Content.....	5
210.9	Supervisory Review of Investigative Documents.....	5
	A. Objective One: Produce Quality Reports	5
	B. Objective Two: Long-Term Writing Improvement.....	5
210.10	Exhibits.....	5

Table of Contents

223.1 Policy 1

223.2 Reference 1

223.3 Scope..... 1

223.4 Definitions 1

 A. Persons in Custody 1

 B. (b) (7)(E), (b) (7)(F) 1

 C. (b) (7)(E), (b) (7)(F) 2

 D. Principal..... 2

 E. Authorized Dependent..... 2

 F. Witness Control Number 2

 G. Sponsoring Attorney 2

 H. Danger or Threat Area 2

223.5 (b) (7)(E) 2

 A. Required Consultation 2

 B. (b) (7)(E) 3

 C. Authorization 4

 D. Documentation..... 4

 E. Additional Concerns 4

 F. OIG Agents and BOP Regulations 4

 G. Exception to Departmental Approval 5

 H. Inmate Victims of Sexual Abuse 6

223.6 Special Precautions Involving (b) (7)(E), (b) (7)(F) 6

 (b) (7)(E), (b) (7)(F)

223.7 (b) (7)(E)

223.8 (b) (7)(E) 8

223.9 (b) (7)(E) 8

223.10 Procedures Governing Persons Taken Into the Custody of the IG 9

223.11	(b) (7)(E) [REDACTED]9
	A. Proposal for Use	9
	B. Conditions of Use	10
	C. Agreement.....	10
223.12	(b) (7)(E) [REDACTED] 10
223.13	(b) (7)(E) [REDACTED] 11
APPENDIX A.	(b) (7)(E) [REDACTED]	.12
APPENDIX B.	(b) (7)(E) [REDACTED] 13
APPENDIX C.	Definitions of Terms In the Prison Rape Elimination Act	14

Table of Contents

226.1	Policy	1
226.2	Reference	1
226.3	Scope.....	1
226.4	General Procedures	1
	A. Federal Law and Administrative Decisions.....	1
	B. Warnings Before Interview.....	1
	C. Representation	1
	D. Instructions to Maintain Confidentiality.....	2
226.5	Collective Bargaining Agreements and the Role of Employee Unions	2
	A. Union Representatives in OIG Interviews	2
	B. Prerequisites for Union Representation at an OIG Interview	3
	C. Role of Union Representative.....	4
226.6	Interviews During Criminal Investigations	5
	A. Definition of a Subject.....	5
	B. Use of Warning Forms.....	5
	C. Refuting Claims of Coercion	5
	D. Custodial Interrogation of Subjects	6
	E. Non-Custodial Interrogation of Subjects in Criminal Investigations	6
	F. Interviews of Witnesses	7
226.7	Interviews During Administrative Investigations.....	8
	A. Definition of a Subject.....	8
	B. Grants of Immunity.....	8
	C. Scheduling Administrative Interviews	8
	D. Warning Forms	9
	E. Scope of Immunity	9
	F. Request for Counsel.....	9
	G. Employee Refusal to Cooperate	10
	H. Off-Duty Conduct.....	11
226.8	Photographic Lineup Displays.....	11
	A. Guidelines for Assembly of the Photo Lineup	11
	B. Conducting a Photo Lineup	12
	C. Recording the Identification Process	12
	D. Evidence	13
226.9	OIG Office of General Counsel Guidance.....	13

226.10	Interviews of Witnesses and Subjects in OIG Office Space.....	13
A.	Instructions Regarding Weapons and Scheduling Interviews	13
B.	Admittance of Witnesses into OIG Office Space	13
C.	Admittance of Subjects into OIG Office Space.....	14
226.11	Interviews of Subjects Outside of OIG Office Space.....	15
A.	Scheduling of Subject Interviews	15
B.	Location of the Interview.....	15
C.	Authority to Modify Policy	16
226.12	Rescheduling of Canceled Interviews	16
226.13	Interviews of Witnesses Outside of OIG Office Space	16
226.14	Interviews at Bureau of Prisons Institutions.....	16
A.	Accommodation of OIG Agents.....	16
B.	Exceptions to Accommodation of OIG Agents	17
C.	Risks of Being Armed in Administrative Areas	17
D.	(b) (7)(E)	17
226.15	Interviews Related to Allegations of Sexual Abuse in Confinement Settings	17
A.	Victim Interviews	17
B.	Subject Interviews	19
APPENDIX A – Acknowledgment of Directive to Maintain Confidentiality and Nondisclosure		20
APPENDIX B – Advisory to Union Representatives.....		21
APPENDIX C – Advisory to Employee After Union Representative Interference With OIG Interview		22
APPENDIX D – Miranda Warnings for Custodial Situations		23
APPENDIX E – Warnings for Non-Custodial Situations – Federal Employees		24
APPENDIX F – Warnings for Non-Custodial Situations – Presidential Appointees.....		25
APPENDIX G – Warnings and Assurances to Employees Required to Provide Information...26		
APPENDIX H – Guide for Employee Interview Situations.....		27
APPENDIX I – OIG OGC Memoranda Relative to Interview Procedures		28
APPENDIX J – Accommodation Requests by OIG Investigators		29
APPENDIX K – Definitions of Terms in the Prison Rape Elimination Act.....		30

Table of Contents

230.1	Policy.....	1
230.2	Reference.....	1
230.3	Scope.....	1
230.4	General Procedures.....	1
230.5	INV-Issued Subpoenas.....	1
	A. Sensitive Targets Exception.....	2
	B. Reimbursement Requests.....	2
	C. Nondisclosure.....	2
	D. Telephone and Internet Requests Beyond Basic Subscriber Information.....	2
230.6	INV-Issued Subpoena Procedures.....	2
	A. Cover Letter.....	2
	B. Subpoena.....	3
	C. Return of Service.....	3
	D. Subpoena Attachment.....	3
	E. Privacy Act Statement.....	4
	F. Certificate of Compliance.....	4
	G. Approval of Subpoena.....	4
	H. Subpoena Numbering System.....	4
	I. Recordkeeping.....	4
230.7	OGC-Issued Subpoenas.....	4
	A. Requesting the Subpoena.....	5
	B. Financial Institutions and Credit Card Issuers.....	5
	C. Credit Reporting Services.....	5
	D. Telephone Companies and Internet Service Providers.....	6
	E. Internal Revenue Service.....	6
	F. State or Public Agencies.....	6
	G. Federal Agencies.....	6
230.8	Service of Subpoenas.....	6
	A. Personal Service Preferred.....	6
	B. Additional Acceptable Methods of Service.....	7
	C. Receipts.....	7
	D. Attorneys.....	8
230.9	Return of Service.....	8
	A. Requirements.....	8
	B. Service by Mail.....	8

230.10	Modification of Subpoenas.....	8
230.11	Production of Records	8
	A. Personal Appearance	8
	B. Original Documents.....	9
	C. Inventorying and Safeguarding Subpoenaed Records.....	9
	D. Certificate of Compliance.....	9
	E. Return of Subpoenaed Records	9
	F. Non-Compliance.....	9
230.12	Privileges Against Disclosure of Records	10
	A. Self-Incrimination (Fifth Amendment).....	10
	B. Attorney-Client Privilege.....	10
230.13	Special Procedures under the Right to Financial Privacy Act.....	11
	A. When the RFPA Applies	11
	B. Obtaining Records With Customer Consent.....	11
	C. Obtaining Customer Records Without the Customer's Consent.....	11
	D. Delayed Customer Notification	13
230.14	Reimbursement to Financial Institutions.....	13
	A. Rates	13
	B. Payment Process	13
230.15	Electronic Communications Privacy Act (ECPA).....	14
230.16	Parallel Proceedings.....	14
	A. Pre-Referral to Prosecutor	14
	B. Post Referral to Prosecutor but Pre-Grand Jury	14
	C. Post Referral to Grand Jury	14
	APPENDIX A. Cover Letter for Field-Issued Subpoenas.....	15
	APPENDIX B. IG Subpoena.....	17
	APPENDIX C. Return of Service.....	19
	APPENDIX D. Sample Language for Field-Issued Subpoenas	21
	APPENDIX E. Privacy Act Notice	24
	APPENDIX F. Certificate of Compliance.....	27
	APPENDIX G. Request Form and Checklist for Field-Issued Subpoenas	29
	APPENDIX H. Field Office Subpoena Log.....	32

APPENDIX I. Sample of an Application for Subpoena Requested Through the Office of General Counsel34

APPENDIX J. Examples of Additional Subpoena Documents to be Completed by OGC37

Table of Contents

231.1	Policy.....	1
231.2	Reference.....	1
231.3	Scope	1
231.4	Grand Jury Materials	1
	A. Limitations on Use	1
	B. Limitations on Access	1
	C. Safeguarding Grand Jury Material	2
231.5	Federal Tax Information.....	2
	A. Limitations on Access and Use	2
	B. Safeguarding Federal Tax Information	3
231.6	Protected Health Care Information.....	4
	A. Limitations on Access and Use	4
	B. Safeguarding Medical Records	4
231.7	Reporting Requirements.....	4
231.8	Protection Standards for National Security Information.....	5

Table of Contents

234.1	Policy	1
234.2	Reference	1
234.3	Scope.....	1
234.4	General Evidence Considerations.....	1
234.5	Evidence Responsibilities.....	1
	A. Agency Responsibilities	1
	B. Individual Responsibilities	1
234.6	Evidence Custodians.....	2
	A. Appointment and Oversight.....	2
	B. Duties and Responsibilities.....	2
234.7	Evidence Holding Facility Security.....	2
	A. Physical Security	2
	B. Access Control.....	3
	C. Storage of OIG Weapons in Evidence Facilities	3
234.8	Evidence Accountability Procedures	3
	A. Seizing Evidence — General Procedures	3
	B. Evidence Custody Document	4
	C. Evidence Logs	6
	D. Evidence Bags	6
234.9	Evidence Storage and Inventory Procedures	6
	A. Storage Procedures	6
	B. Special Storage Problems	6
	C. Evidence Inventories	7
234.10	Special Considerations Regarding Genuine Currency	7
	A. Seizing and Counting Genuine Currency	8
	B. Joint Investigation Seizures	8
	C. Defendants in Possession of Genuine Currency.....	8
	D. Seizures of Large or Unusual Amounts of Cash	9
	E. Forfeiture of Money to Cover Fines or Victim Compensation.....	9
	F. Storage of Genuine Currency Pending Final Disposition.....	10
234.11	Evidence Shipment Procedures	10
	A. Packaging.....	10
	B. Shipment Between DOJ OIG Offices.....	10
	C. Shipment to Laboratories.....	10

234.12	Evidence Disposition	10
A.	Release of Evidence for Trial	10
B.	Return of Evidence to Owner	11
C.	Final Disposition Guidelines	11
D.	Disposition of Bribe Monies and Other Genuine Currency	13
E.	Procedures for Requesting Approval for Direct Deposit to the U.S. Treasury	14
F.	Procedures for Transmitting Bribe Monies or Other Genuine Currency	14
G.	Prolonged Evidence Retention	15
234.13	Special Evidentiary Considerations Regarding Investigations of Sexual Abuse in Confinement Settings.....	15
A.	Initial Preservation of Evidence.....	15
B.	Medical Examinations	16
C.	Conducting Forensic Crime Scene Investigation Involving Biological Evidence	16
D.	Handling Biological Evidence.....	17
E.	Detecting and Testing Forensic Evidence	17
APPENDIX A.	Evidence Custody Document (OIG Form III-234/1) Evidence Disposition Document (OIG Form III-234/4)	
APPENDIX B.	Investigations Division Evidence Log (OIG Form III-234/2)	
APPENDIX C.	Evidence Bag Seal and Label	
APPENDIX D.	Sample Memorandum Request to Dispose of Seized Funds	
APPENDIX E.	Transmittal of Bribe Monies (OIG Form III-234/3) Transmittal of Bribe Monies — Continuation (OIG Form III-234/3A)	
APPENDIX F.	Definitions of Terms in the Prison Rape Elimination Act	

Table of Contents

300.1	Policy.....	1
300.2	References	1
300.3	Scope	1
300.4	Definitions	1
	A. Serious Incident.....	1
	B. Traumatic Incident	1
	C. Post-Traumatic Stress Disorder.....	1
	D. Agent-Involved Shooting Incident	2
300.5	Responsibilities in the Event of a Serious Incident.....	2
	A. Notification by Employee	2
	B. Field Supervisor	2
	C. INV Headquarters.....	2
300.6	Procedures.....	3
	A. Shooting Incident Procedures.....	3
	B. After-Incident Procedures	5
	C. Injured Agent Procedures.....	6
	D. Management Follow-Up.....	6

Table of Contents

Table of Contents..... 1

003.1 Policy.....2

003.2 Reference.....2

003.3 Scope.....2

003.4 Procedures.....2

003.5 Responsibilities.....2

003.6 Continuity of Operations4

Table of Contents

270.1	Policy.....	1
270.2	References.....	1
270.3	Scope.....	1
270.4	Responsibilities.....	1
	A. The Inspector General.....	1
	B. The Human Resources Officer.....	1
	C. Reviewing Officials.....	2
	D. Rating Officials.....	2
270.5	Appraisal Period.....	2
270.6	Performance Rating System.....	3
270.7	Performance Work Plans.....	3
270.8	Progress Reviews.....	4
270.9	Annual Performance Appraisal.....	4
	A. Appraising Performance in Special Circumstances.....	4
	B. Assignment and Documentation of Rating Levels.....	5
	C. Determination and Documentation of Summary Overall Rating.....	6
	D. Approval by Reviewing Official.....	7
270.10	Actions Based on Performance Ratings.....	7
	A. Award Recognition.....	7
	B. Actions Based on Overall Rating of "Unacceptable.".....	7
	C. Performance Improvement Plans.....	8
	D. Employee Challenges of Performance Ratings.....	8
270.11	Performance Management Records.....	8
270.12	Program Evaluation.....	8
270.13	Program Changes and Revisions.....	8

Table of Contents

295.1	Purpose.....	1
295.2	Scope.....	1
295.3	Authority.....	1
295.4	Policy.....	1
295.5	Definitions.....	1
	A. Adverse Action.....	1
	B. Major Adverse Action.....	1
	C. Office Heads.....	1
295.6	Responsibilities.....	1
	A. The Inspector General.....	1
	B. The Deputy Inspector General.....	1
	C. The Assistant Inspectors General.....	2
	D. The Assistant Inspector General, Management and Planning Division.....	2
	E. The Deputy Assistant Inspectors General.....	2
	F. Office Heads.....	2
	G. General Counsel.....	2
	H. Personnel Officer.....	2
	I. Supervisors and Managers.....	3
	J. Employees.....	3
295.7	Authority to Propose and/or Decide Disciplinary Actions.....	3
	A. General.....	3
	B. Official Reprimands.....	3
	C. Suspensions of 14 days or less.....	3
	D. Major Adverse Actions.....	3
	E. Adverse Actions for Attorneys.....	4
295.8	Review of Actions.....	4
295.9	Maintenance of Case Records.....	4
295.10	Home Duty Status.....	4
	A. Conditions.....	4
	B. Authority.....	4
	C. Activity.....	4
APPENDIX A.....		7

Table of Contents

003.1	Policy	1
003.2	Reference	1
003.3	Scope.....	1
003.4	Procedures.....	1
003.5	Responsibilities.....	1
003.6	Continuity of Operations	3

Table of Contents

211.1	Purpose	1
211.2	Scope.....	1
211.3	Authority.....	1
211.4	Policy	1
211.5	Definitions	1
	A. Designated Official	1
	B. Occupant Emergency Organization (OEO).....	1
	C. Occupant Emergency Plan (OEP)	1
	D. Prime Tenant.....	1
	E. Security Programs Manager	1
211.6	Occupant Emergency Organization	1
	A. General.....	1
	B. Central Command Team.....	1
	C. Floor Teams	3
	D. Damage Control Teams	4
211.7	Occupant Emergency Plan.....	4
	A. Responsibility	4
	B. Contents	4
	C. Initiating Action.....	5
	D. Review	5
	E. Availability	6

Table of Contents

105.1	Policy.....	1
105.2	Reference.....	1
105.3	Scope.....	1
105.4	Establishing and Maintaining the OIG Vehicle Fleet.....	1
	A. Assignment of Vehicles.....	1
	B. Operating Costs.....	2
	C. Service, Maintenance, and Repair Costs.....	3
	D. Vehicle Registration Costs.....	4
	E. Documenting and Tracking Costs.....	4
	F. Equipment to be Carried in OIG Vehicles.....	4
105.5	Government Vehicle Use Policy.....	5
	A. General Provisions.....	5
	B. Parking and Traffic Violations.....	7
	C. Vehicle Accidents (Including Vandalism and Road Hazard Damage).....	7
	D. Physical Fitness Report.....	10
105.6	Record Keeping Requirements for OGVs.....	11
	A. Official Government Vehicle Monthly Log.....	11
	B. Monthly Vehicle Report Summary.....	11
	C. OGV Fleet Summary Spreadsheet.....	11
105.7	Home-to-Work Use of OGVs.....	12
	A. Who May Use an OGV for Home-to-Work.....	12
	B. Limitations.....	12
	C. Certification Procedures.....	12
	D. Decertification.....	13
	E. Record Keeping Requirement for Home-to-Work OGV Use.....	13
105.8	Emergency Driving.....	13
	A. Definition.....	13
	B. Authorization.....	13
	C. Prohibition.....	13
	D. Planning.....	14
	E. Authorized Emergency Equipment.....	14
	F. Use of Emergency Equipment.....	14
	G. Continuing Responsibility.....	14
	H. Mandatory Factors for Consideration.....	15

I.	Termination of Pursuit.....	15
J.	Maneuver Tactics During Pursuit.....	15
K.	Liability	16
L.	Joint Operations.....	16
105.9	Environmental Management Plan	16
A.	General	16
B.	Fuel and Maintenance	16
C.	Alternate Fuel Vehicles	16
D.	Energy Conservation	16
E.	Reporting	17
F.	Continuing Improvement	17
105.10	Texting While Driving.....	17
A.	Definitions	17
B.	Prohibition	18
C.	Authorized Exemptions.....	18
APPENDIX A.	Home-to-Work Transportation Action Plan	20
APPENDIX B.	Official Government Vehicle Monthly Log	24
APPENDIX C.	Monthly Vehicle Report Summary	27
APPENDIX D.	Sample Official Government Vehicle Fleet Summary Spreadsheet.....	30
APPENDIX E.	Certification for Home-to-Work Use of Official Government Vehicle.....	32

Table of Contents

110.1 Policy 1

110.2 Reference 1

110.3 Scope..... 1

110.4 Responsibilities..... 1

 A. Special Agent in Charge, Investigative Support Branch, Investigations Division
 Headquarters 1

 B. Special Agent in Charge, OIG Field Office..... 1

 C. Assistant Special Agent in Charge 2

 D. Special Agent Coach..... 3

 E. New Special Agent 3

110.5 New Special Agent Development Program 4

 A. Phase One 4

 B. Phase Two..... 4

110.6 Assignment of a Coach 5

110.7 Formal Training Requirements 5

 A. Basic Training..... 5

 B. IG Academy 6

 C. Interviewing Techniques 6

 D. Other Training 6

110.8 Continuing Education Requirements 6

110.9 Training for Senior Special Agents 7

110.10 Training for ASACs and SACs..... 7

 A. Human Resources Management 7

 B. Basic Supervision 7

 C. Equal Employment Opportunity (EEO) for Managers and Supervisors 7

APPENDIX A 8

APPENDIX B 9

APPENDIX C 10

APPENDIX D 11

APPENDIX E 12

Table of Contents

201.1	Policy	1
201.2	Reference	1
201.3	Scope.....	1
201.4	Responsibilities.....	1
	A. Inspector General.....	1
	B. Assistant Inspector General for Investigations	1
	C. Special Agent in Charge, Investigative Support Branch, Investigations Division Headquarters	1
	D. SACs of Field Offices.....	1
	E. Special Agent.....	2
201.5	Issuance of Firearms	3
201.6	Carrying Firearms.....	4
	A. On Duty	4
	B. Off Duty.....	4
	C. Regulations and Policies Regarding Handling Firearms	4
	D. (b) (7)(E)	5
	E. In Federal Prisons and Courthouses	6
	F. OIG Agents and Domestic Violence	7
201.7	Prohibited Acts	7
201.8	Use of Deadly Force	7
201.9	OIG-Approved Firearms.....	7
	A. Primary Duty Handgun.....	7
	B. Auxiliary Handgun	9
	C. OIG-Approved Shoulder Weapon	10
201.10	Firearms Care.....	10
201.11	Transportation and Shipment.....	10
201.12	Ammunition	10
201.13	Loss of Weapon	11
201.14	Handling and Storage of Weapons	11

A.	Handgun Storage in an OIG Office	11
B.	Handgun Storage in the Home.....	11
C.	Field Office Stored Shoulder Weapons and Other Unissued OIG Firearms	11
D.	Loaded weapons	12
E.	Loading and Unloading Firearms	12
F.	Dry Firing	12
201.15	Firearms Discharges – Reporting Requirements	12
A.	Shooting Incidents	12
B.	Accidental Firearm Discharges.....	13
201.16	Response Requirements After a Shooting Incident	14
201.17	Shootings and Critical Incidents Review.....	15
201.18	Legal Representation	15
A.	Scope of Employment.....	15
B.	Interest of the United States.....	15
C.	Criminal Liability	16
D.	Civil Liability Under the Federal Tort Claims Act.....	16
E.	Civil Liability for Constitutional Violations.....	17
F.	Representation for Incidents Involving Enforcement of State Laws	17
G.	Procedures for Obtaining DOJ Legal Representation	18
H.	Emergency Interim Legal Representation	18
201.19	Holsters	20
A.	Belt Holsters	20
B.	Alternate Holsters	20
201.20	Firearms Training and Qualification – General Considerations	21
A.	Training Days	21
B.	Ranges.....	22
C.	Area Offices.....	22
201.21	Firearms Training and Qualification Courses.....	22
A.	Firearms Instructors	22
B.	Initial Training and Qualification	22
C.	Pistol Qualification Course.....	23
D.	RESERVED.....	23
E.	Rifle Qualification Course.....	23
F.	Auxiliary Qualification Course.....	23
201.22	Recording and Reporting Firearms Training and Qualification	24
A.	The Weapons and Related Training Card.....	24
B.	Quarterly Firearms Qualification and Training Report	25

201.23	Handling Failure to Qualify Situations.....	25
	A. Failure to Attend Firearms Qualification.....	25
	B. Failure to Achieve Minimum Qualification Score	26
201.24	Defensive Tactics Program.....	27
201.25	Reality-Based Training.....	30
201.26	Recording and Reporting Defensive Tactics or Reality-Based Training	31
APPENDIX A.	Weapons and Related Training Card	32
APPENDIX B.	Sample Quarterly Firearms Qualification and Training Report.....	34
APPENDIX C.	DOJ Policy Statement – Use of Deadly Force	36
APPENDIX D.	Ammunition Log.....	40
APPENDIX E.	Rifle Log.....	42
APPENDIX F.	Firearm Discharge/Assault Report	41
APPENDIX G.	OIG Form III-201/5 (Use of Non-Lethal Force Report).....	42
APPENDIX H.	Department of Justice Less Than Lethal Use of Force Policy	51

Table of Contents

202.1	Policy	1
	A. OIG Employees	1
	B. OIG Witnesses and Victims of Crime	1
202.2	Reference	1
202.3	Scope.....	1
202.4	Definitions	2
	A. Covered OIG Employees	2
	B. Victim	2
	C. Witness	2
	D. Serious Crime (As Used in the Victim Witness Protection Act of 1982).	2
202.5	Procedures Regarding Threats or Assaults Against Covered OIG Employees.	2
	A. Initial Actions to Be Taken.....	2
	B. Reporting Threats or Assaults	3
	C. Relocation of Employee	3
	D. Injury or Death of a Covered Employee.....	4
202.6	Procedures Regarding Threats or Assaults Against OIG Witnesses	4
	A. Initial Actions to Be Taken.....	4
	B. Reporting Threats or Assaults	4
	C. Relocation of the Witness.....	5
202.7	Victim/Witness Assistance When No Immediate Threat Exists	5
202.8	The OIG Victim/Witness Assistance Program	6
	A. Victim/Witness Coordinator.....	6
	B. Case Agent Responsibilities	8
	C. SAC Responsibilities	9
	D. Investigations Division Headquarters Responsibilities	9
	E. (b) (7)(E)	9
202.9	Warning Persons and Notifying Law Enforcement Agencies of Threats to Life or Serious Bodily Injury.....	10
	A. Warning the Threatened Individual	10
	B. Exceptions.....	10
	C. Notifying Other Law Enforcement Agencies	10
	D. Documentation.....	11
202.10	(b) (7)(E), (b) (7)(F)	11
	A. Criteria	11

B. Procedures.....	12
(b) (7)(E), (b) (7)(F)	
APPENDIX A.....	16

Table of Contents

221.1	Policy	1
221.2	Reference	1
221.3	Scope.....	1
221.4	Authorization Process for Foreign Travel on Official Business.....	1
	A. Alternatives to Foreign Travel.....	1
	B. Approvals Required	1
	C. Application Requirements	2
221.5	Official Passports and Visas	3
	A. Official Passport Required.....	3
	B. Visas	4
221.6	U.S. Government Travel Regulations.....	4
	A. General Services Administration.....	4
	B. Immigration and Customs Enforcement.....	4
221.7	Investigative Authority and Conduct of OIG Personnel While Overseas	4
	A. Jurisdiction.....	4
	B. (b) (7)(E)	4
	C. (b) (7)(E)	4
	D. Diplomatic Concerns	5
	E. Liability for Actions Overseas.....	5
APPENDIX A.....		7

Table of Contents

224.1	Policy	1
224.2	Reference	1
	A. Examples of Complaints.....	1
	B. DOJ Civil Rights Division.....	1
	C. IDMS II Civil Rights Field.....	2
	D. IDMS II Classification.....	2
	E. Recording the CRD/USAO Decision in IDMS II.....	3
	F. CRD and USAO Declination.....	3
	G. USAO Interest	3
	H. CRD Interest	3
	I. OIG or Joint Investigation	3
	J. FBI Investigation	3
224.5	Managing and Investigating Civil Rights Complaints — General.....	4
	A. Federal Civil Rights Statutes	4
	B. The USA Patriot Act of 2001	5
	C. Coordination and Liaison Responsibilities.....	5
	D. Administrative Investigations.....	6
224.6	Investigating Civil Rights Complaints — Investigative Steps	6
	(b) (7)(E)	
	APPENDIX A.....	11

Table of Contents

232.1	Policy	1
	A. Arrest Warrant	1
	B. (b) (7)(E)	1
232.2	Reference	1
232.3	Scope.....	1
232.4	Obtaining an Arrest Warrant	1
	A. Coordination With Prosecutor	1
	B. Warrant Application	1
	C. Probable Cause	2
	D. Venue.....	2
	E. Forms	2
232.5	Planning the Arrest	2
	A. Safety	2
	B. Command.....	2
	C. Arrest Plan	2
	D. Pre-Arrest Briefing	3
	E. Locating the Potential Arrestee	3
232.6	Notification and Coordination Before Arrest	3
	(b) (7)(E)	
232.7	Arrest Procedures.....	3
	A. General Considerations.....	3
	B. Location of Arrest.....	4
	C. Use of Force.....	5
	D. Searches Conducted Incidental to the Arrest.....	5
	E. Handcuffing	6
	F. Miranda Warnings	6
232.8	Transporting Arrestees.....	7
232.9	Medical Attention for Arrestees	7
232.10	Processing Arrestees	7
	A. Processing Location.....	8
	B. Obtaining Personal History.....	8
	C. Interviewing	8

D.	Photographs	9
E.	Fingerprinting	9
F.	DNA Collection	9
G.	Personal Property	10
H.	Initial Appearance	10
232.11	Arrest of Juveniles	11
232.12	Arrest of Foreign Nationals	11
232.13	Arrests Without a Warrant	12
A.	Permissible On-Duty Arrest	12
B.	Other Permissible Situations	12
C.	Required Procedures	12
D.	Liabilities	13
232.14	Post-Arrest Reporting and Notification	13
A.	Internal Reporting of Any Arrest Made by an Agent	13
B.	Notification of the Prosecutor and Coordination of the Press Release	14
232.15	Arrest Credit Criteria	14
A.	OIG Investigation	14
B.	Joint Investigation	15
C.	Fugitives/Wanted Persons	15
APPENDIX A.	Arrest Plan Format	16
APPENDIX B.	Personal History Report	17
APPENDIX C.	Criminal Fingerprint Card and Final Disposition Report	18
APPENDIX D.	OIG Originating Agency Identifier Numbers	19
APPENDIX E.	Statement to Arrested Foreign Nationals When Notification Is Optional and Statement to Arrested Foreign Nationals When Notification Is Mandatory	20
APPENDIX F.	Required Consular Notification of Arrests of Foreign Nationals	21
APPENDIX G.	Attorney General Weekly Report Guidelines and Sample Submissions	22

Table of Contents

233.1	Policy	1
233.2	Reference	1
233.3	Scope.....	1
233.4	Definitions	1
	A. Search	1
	B. Seizure	1
	C. Particularity.....	1
	D. Probable Cause	1
	E. Reasonable Suspicion	1
	F. Plain View Doctrine	2
	G. Abandonment.....	2
	H. Exclusionary Rule.....	2
	I. Contraband.....	2
233.5	Searches With Warrants	2
	A. Fourth Amendment Protections.....	2
	B. Federal Rules	2
233.6	Obtaining the Search Warrant	2
	A. Requirements	2
	B. Items Subject to Seizure	3
	C. Persons Authorized to Serve a Search Warrant.....	4
	D. Timing of Execution	4
	E. Nighttime Searches	4
	F. Obtaining a Search Warrant Upon Oral Testimony	4
233.7	Executing the Search Warrant	5
	A. Planning the Service	5
	B. Gaining Entry to Premises	5
	C. (b) (7)(E)	6
	D. Search Procedures.....	6
	E. Inventory of Seized Items.....	7
	F. Noting Date and Time	8
233.8	Reporting the Search.....	8
233.9	Searches Without Warrant.....	8
	A. Search Incident to Arrest	8
	B. Limited Protective Search (Frisk).....	8
	C. Consent Search	9

D.	Emergency Searches	10
E.	Abandoned Property	11
F.	Vehicle Searches.....	11
233.10	Special Situations.....	12
A.	Government Workplace Searches.....	12
B.	Searches Involving Seizure of Electronic Records and Computers	12
C.	Searches Involving Seizure of Mobile Devices, Cell Phones and Smartphones...	13
D.	Use of Auditors/Inspectors	14
E.	Non-Federal Crimes.....	15
F.	Freezing Premises Pending Issuance of a Search Warrant.....	15
G.	Searches of Inmates or Inmate Space in Federal Prisons	16
APPENDIX A.	Sample Affidavit in Support of Search Warrant	17
APPENDIX B.	Sample Search Plan	18
APPENDIX C.	Search Briefing Guide	19
APPENDIX D.	Receipt for Cash or Other Items	27
APPENDIX E.	Consent to Search Premises/Vehicle, Consent to Collect a DNA Reference Sample	21
APPENDIX F.	Sample Affidavit in Support of Search Warrant Application for Computer Equipment	22
APPENDIX G.	Consent to Search Computer/Electronic Equipment	23

Table of Contents

235.1	Policy	1
235.2	Reference	1
235.3	Scope.....	1
235.4	General.....	1
	A. Case Initiation.....	1
	B. Case Closing.....	1
	C. Evidence Handling.....	1
	D. Use of Outside Laboratories.....	2
	E. Biohazard.....	2
235.5	Forensic Media Analysis	2
	A. Responsibilities and Oversight	2
	B. Selection and Training of CFAs	6
	C. Authorized Forensic Media Analysis	7
	D. Requesting Forensic Media Analysis	7
	E. Forensic Media Analysis Procedures.....	9
	F. Reporting Forensic Media Analysis	9
235.6	Computer Intrusion Investigations	9
	A. Initial Response	9
	B. Investigative Response Consideration Criteria.....	10
	C. Tracking Intrusion Activity	11
	Appendix A. Digital Forensic Examination Request	12

Table of Contents

240.1 Policy 1

240.2 Reference 1

240.3 Scope..... 1

240.4 Definitions 1

 A. Attorney General Guidelines 1

 B. Chief Federal Prosecutor 1

 C. Confidential Informant 1

 D. Confidential Informant Review Committee 1

 E. Cooperating Witness..... 2

 F. Federal Prosecuting Office 2

 G. Fugitive 2

 H. High Level Confidential Informant 2

 I. Source of Information..... 3

 J. Target..... 3

 K. Tier 1 Otherwise Illegal Activity 3

 L. Tier 2 Otherwise Illegal Activity 3

240.5 Responsibility for Development and Control of CIs 4

 A. Confidential Informant Program Manager 4

 B. Special Agent in Charge 4

 C. Confidential Informant Coordinator 4

240.6 (b) (7)(E) 4

240.7 Establishing a Confidential Informant..... 4

 A. Initial Suitability Assessment 4

 B. Suitability Assessment and Recommendation Form 7

 C. Prohibition against Payments or Benefits Prior to Registration 7

 D. Approvals..... 7

240.8 Informant Debriefing 8

 A. Information to Be Sought From Informants 8

 B. Dissemination of Criminal Information Received 8

 C. Debriefing Memorandum 8

240.9 Registering a Confidential Informant 8

 A. Personal History Report..... 9

 B. Suitability Assessment and Recommendation 9

 C. Criminal Records Check and Informant History Check..... 9

 D. Financial Records Check 9

 E. Photographs and Fingerprints 10

	F. Acknowledgement of Informant Instructions.....	10
	G. Distribution.....	10
240.10	Guidelines and Instructions to Be Discussed With a CI.....	10
240.11	(b) (7)(E)	
240.12	Informant Files.....	12
	A. Required Contents of Informant Files	13
	B. The Headquarters Informant File and Database	13
	C. File Storage.....	14
240.13	Annual CI Suitability Review.....	14
	A. Administrative Requirements	14
	B. Review Questions to Be Answered	14
	C. Documentation.....	15
240.14	Suitability Review for (b) (7)(E)	15
	A. CIRC Review.....	15
	B. Internal OIG Review.....	15
240.15	Security and Storage of Informant Information and Files	15
	A. File Segregation and Security	15
	B. Protecting the CI's Identity.....	16
240.16	Special Requirements and Approvals	16
	(b) (7)(E)	
240.17	CI Participation in Otherwise Illegal Activity.....	21
	A. General Provisions.....	21
	B. Authorization	21

	C.	Findings	22
	D.	Instructions to the CI	23
	E.	Precautionary Measures	24
	F.	Emergency Authorization	24
	G.	Suspension of Authorization	25
	H.	Revocation of Authorization	25
	I.	Renewal or Expansion of Authorization	26
240.18		Notification of Unauthorized Illegal Activity	26
	A.	Chief Federal Prosecutor	26
	B.	State or Local Prosecutor	26
	C.	CI File	26
	D.	CIPM	27
240.19		Protecting CI Confidentiality, Disclosures, and Special Notifications	27
	A.	Policy	27
		(b) (7)(E) [REDACTED]	
	L.	Continuing Obligation to Maintain Confidentiality	31
240.20		Entry of Foreign Nationals Into the United States as Informants	31
	A.	Significant Public Benefit and Humanitarian Parole	31
	B.	The "S" Visa Program	32
240.21		Specific Guidelines for Using CIs	33
240.22		Informant Compensation	34
	A.	Payment Guidelines	34
	B.	Compensating Other Agency Informants	35
240.23		Payment Authorizations	35
	A.	Single Payments	35
	B.	Aggregate Payments	35
	C.	Documentation	35
	D.	Accounting for CI Payments	36
240.24		Informants (b) (7)(E), (b) (7)(F) [REDACTED]	36
	A.	(b) (7)(E), (b) (7)(F) [REDACTED]	36

B.	Short Term or Interim Reimbursement.....	36
240.25	Use of Polygraph	36
240.26	Deactivation of Informants	36
A.	Standard Deactivation.....	36
B.	Deactivation for Cause	36
C.	Deactivation Debriefing.....	37
D.	Documentation.....	37
E.	Coordination with Prosecutors	37
240.27	Reactivation of Informants	38
240.28	Exceptions to the Attorney General Guidelines and Dispute Resolution.....	38
APPENDIX A	39
APPENDIX B	40
APPENDIX C	41
APPENDIX D	42
APPENDIX E	43
APPENDIX F	44
APPENDIX G	45

Table of Contents

250.1	Policy	1
	A. Objectives	1
	B. Undercover Techniques	1
	C. Undercover Conduct Coordination and Policy Compliance	1
	D. Non-Agent OIG Personnel and Cooperating Persons	1
250.2	Reference	2
250.3	Scope	2
250.4	Definitions	2
	A. Undercover Operative	2
	B. Undercover Activity	2
	C. Undercover Operation	2
	D. Proprietary	3
	E. Contact Agent	3
250.5	Planning and Initiating Undercover Operations	3
	A. Preliminary Planning	3
	B. Coordination with INV Headquarters	3
	C. Identification and Selection of Individuals to Work in an Undercover Capacity	4
	D. Undercover Documents	4
	E. Emergency and Security Considerations	4
	F. Operational Plan	5
	G. Operations Meeting	5
250.6	Authorization for Undercover Activities and Operations	6
	A. SAC	6
	B. AIG/I	6
	C. Undercover Operations Involving Sensitive Circumstances	7
	D. Undercover Operations Involving Special Fiscal Circumstances	7
	E. Required DOJ Office of Enforcement Operations Approval	8
250.7	Application to Headquarters	8
	A. Scope and Objectives	8
	B. Cover	8
	C. Informants	8
	D. Risks	8
	E. Offense	8
	F. Anticipated Duration	8
	G. Estimate of Resources	8
	H. Sensitive and Fiscal Circumstances	8
	I. Federal Prosecutor	9
	J. Changes in Scope or Objectives	9

250.8	Emergency Authorization.....	10
	A. SAC Approval	10
	B. Sensitive Circumstances.....	10
	C. Written Application	10
	D. Application Denial	10
250.9	Reserved	10
250.10	Undercover Operations Application and Review Process	10
	A. Special Fiscal Circumstances	10
	B. Sensitive Circumstances.....	11
	C. Factors	11
	D. Approval.....	11
	E. Joint Investigations.....	11
	F. Notifications	12
250.11	Participation in “Otherwise Illegal” Activity	12
	A. Factors	12
	B. Approvals Required.....	12
	C. Minimized Participation	12
	D. Prohibited Acts	13
	E. Unanticipated Participation	13
	F. Self-Defense	13
	G. Serious Incident of Violence	13
250.12	Undercover Documents	13
	A. Documents Obtainable at the Field Office Level	13
	B. Documents Obtainable Through Another Field Office	14
	C. Documents Obtainable Through Headquarters	15
250.13	(b) (7)(E)	
250.14	(b) (7)(E)	
250.15	(b) (7)(E)	18

(b) (7)(E)

250.16 Monitoring and Control of Undercover Operations 21

- A. Accounting Procedures..... 21
- B. Monthly Reports..... 21
- C. SAC Responsibilities..... 22
- D. Headquarters Responsibilities 22
- E. Reviews 23
- F. Quarterly Reviews..... 23
- G. Proprietaries..... 24

250.17 File Maintenance for Undercover Operations Authorized by INV Headquarters 24

(b) (7)(E)

250.18 Closing an Undercover Operation 25

- A. Field Office Review 25
- B. INV Headquarters Review 25
- C. Proceeds From an Undercover Operation 25
- D. Proprietary Operations 25

APPENDIX A. Council of the Inspectors General on Integrity and Efficiency Guidelines 27

APPENDIX B. Undercover Policy Flowchart 28

APPENDIX C. Undercover Role and Security Considerations Guide 29

APPENDIX D. Undercover Operations Meeting Guide..... 30

APPENDIX E. Undercover Document Request (OIG Form III-250/1) 31

APPENDIX F. Guide for Field Office Review of Undercover Activity..... 32

Table of Contents

260.1	Policy	1
260.2	Reference	1
260.3	Scope.....	1
260.4	Overview of the Electronic Communications Privacy Act of 1986	1
260.5	Interception of Communications and Related Matters	1
	A. The Electronic Communications Privacy Act of 1986	1
	B. Title III Statute References	2
260.6	Stored Wire and Electronic Communications and Transactional Records Access	2
260.7	Pen Register and Trap and Trace Devices	3
260.8	Responsibilities.....	3
	A. Assistant Inspector General for Investigations	3
	B. Deputy Assistant Inspector General for Investigations	3
	C. Special Agent in Charge, Investigative Support Branch, INV Headquarters.....	3
	D. Special Agents in Charge.....	3
	E. Assistant Special Agent in Charge	3
	F. Special Agents	3
260.9	Definitions	3
	A. Wire Communication.....	3
	B. Oral Communication	4
	C. Intercept	4
	D. Electronic, mechanical, or other device.....	4
	E. Person	4
	F. Investigative or Law Enforcement Officer	4
	G. Electronic Communication	4
	H. Mobile Tracking Device	5
	I. User.....	5
	J. Electronic Communications System.....	5
	K. Electronic Communications Service.....	5
	L. Electronic Storage.....	5
	M. Aural Transfer.....	5
	N. Consensual Conversation.....	5
	O. Nonconsensual Conversation.....	5
	P. Reasonable Expectation of Privacy	5
	Q. Additional Definitions	6
260.10	Exceptions.....	6

(b) (7)(E)

260.11 Storage and Use of Technical Equipment 7

260.12 Telephone Communications 7

260.13 Subscriber/Toll Information 7

260.14 Telephone Decoders 9

260.15 Consensual Telephone Intercepts 11

260.16 Consensual Nontelephone Communication Intercepts 12

 A. Consensual Intercept of Nontelephone Communications 12

 B. Concurrence and Approval 12

260.17 Non-Emergency Procedures for Approving Consensual Nontelephone Communications Intercepts 12

260.18 Emergency Procedures for Obtaining Approval of Consensual Nontelephone Communications 15

260.19 Other Surveillance Operations 16

 A. Mobile Tracking Devices 16

 B. Warrant Authorizing the Monitoring of a Signal 17

 C. Refer Questions 17

260.20 (b) (7)(E) 17

260.21 (b) (7)(E) 18

260.22 Video Surveillance 18

260.23 (b) (7)(E) 18

260.24 (b) (7)(E)

260.25 Video Approval Process 19

260.26	Use of Electronic Surveillance Techniques.....	19
	A. Domestic.....	19
	B. Foreign.....	20
260.27	Electronic Communications.....	20
260.28	Other Protected Electronic Communications	21
	A. Digital Display Pagers	21
	B. Approval Process	21
	C. Restrictions	21
	D. Reporting Process	21
	E. Intercept Completion	22
260.29	Access to Stored Electronic Communications.....	22
	A. The Electronic Communications Privacy Act	22
	B. Providers of Electronic Communication Service vs. Remote Computing Service.....	22
	C. Electronic Storage.....	22
	D. Compelled Disclosure Under the ECPA.....	23
	E. Subpoena.....	23
	F. Subpoena With Notice.....	23
	G. Court Orders and Warrants.....	24
	H. Cost Reimbursement.....	24
260.30	Nonconsensual Telephone Intercepts	24
260.31	Tactical Planning of Court Ordered Intercept of Wire Communications.....	25
260.32	Application for a Court Order to Conduct an Interception of Wire Communication.....	26
260.33	Operation of the Intercept.....	28
	(b) (7)(E)	
260.34	Wire Intercept Procedures	29
260.35	(b) (7)(E)	32
260.36	Master Affidavit.....	33
260.37	Requesting Extensions to a Wire Intercept.....	33
260.38	Terminating the Wire Intercept	33
260.39	Reporting Requirements for Wire Intercepts.....	34
260.40	Nonconsensual Intercepts Other Than Telephone	35

260.41 OIG Form III-260/1 (Title III Intercept Report).....35

260.42 OIG Form III-260/2 (Title III and Pen Register Index).....36

APPENDIX A.....37

APPENDIX B.....38

Table of Contents

265.1	Policy	1
265.2	Reference	2
265.3	Scope.....	2
265.4	Responsibility and Control	2
	A. AIGI.....	2
	B. SAC, Polygraph Program, INV Headquarters.....	2
	C. Polygraph Program Coordinator.....	2
	D. Polygraph Examiner	3
265.5	Case Application.....	4
	A. OIG Investigations.....	4
	B. Other Agency Investigations	5
265.6	Initiating a Polygraph Examination	5
	A. Case Agent Responsibility.....	5
	B. The Polygraph Request.....	6
	C. (b) (7)(E)	7
265.7	Certification and Decertification of OIG Polygraph Examiners	8
265.8	Polygraph Program Quality Control.....	8
265.9	Polygraph Authorization and Reporting Procedures	9
	A. Polygraph Travel Authorization	9
	B. Polygraph Examination Results Notification	9
	C. The Polygraph Examination Report	9
	D. Distribution of Polygraph Examination Reports	10
265.10	Administratively Compelled Polygraph Examinations	10
265.11	Polygraph Examination Files.....	12
265.12	Polygraph Equipment	12
	A. Polygraph Instruments and Related Equipment	12
	B. Polygraph Demonstrations.....	13
265.13	Monitoring Polygraph Examinations.....	13
265.14	Use of Interpreters	13
265.15	Polygraph Examination Statistical Reports	13

APPENDIX A. Request for Polygraph Examination (OIG Form III-265/1) 14

APPENDIX B. Sample Compelled Polygraph Memorandum 15

APPENDIX C. Sample E-Mail for Polygraph Examiner Travel Authorization 16

APPENDIX D. Sample E-Mail – Polygraph Examination Results..... 17

APPENDIX E. Sample Polygraph Examination Report (Pages 1 and 2)..... 18

APPENDIX F. Definitions of Terms in the Prison Rape Elimination Act) 19

Table of Contents

300.1	Policy.....	1
300.2	References	1
300.3	Scope	1
300.4	Definitions.....	1
	A. Serious Incident.....	1
	B. Traumatic Incident	1
	C. Post-Traumatic Stress Disorder.....	1
	D. Agent-Involved Shooting Incident.....	2
300.5	Responsibilities in the Event of a Serious Incident.....	2
	A. Notification by Employee	2
	B. Field Supervisor	2
	C. INV Headquarters.....	2
300.6	Procedures.....	3
	A. Shooting Incident Procedures.....	3
	B. After-Incident Procedures	5
	C. Injured Agent Procedures.....	6
	D. Management Follow-Up.....	6

Table of Contents

3.1	Policy	2
3.2	Reference	2
3.3	Scope.....	2
3.4	Responsibilities	2
	A. The Inspector General (IG).....	2
	B. Assistant Inspectors General (AIGs) and General Counsel (GC).....	3
	C. The Budget Officer, under the direction of the Director, Office of Financial Management	3
3.5	Procedures.....	4
3.6	Timetable of Budget Submissions	4

Table of Contents

020.1	Purpose	1
020.2	Scope.....	1
020.3	Authority.....	1
020.4	Policy	1
020.5	Special Operations Funding	1
	A. Special Operation Support (SOS) Accounts	1
	B. Case Specific Accounts	2
	C. Headquarters Funding.....	2
	D. Equipment and Supplies	2
020.6	Responsibilities and Authorities	2
	A. The AIG/INV	2
	B. The Deputy Assistant Inspector General for Operations (DAIG/OPS).....	2
	C. The Office Head.....	2
	D. The ASAC.....	3
	E. The Deputy Assistant Inspector General for Budget and Planning (DAIG/B&P).....	3
	F. The Financial Manager	3
	G. The Disbursing Officer	3
	H. The Accountable Officer	3
	I. The Budget and Planning (B&P) Staff.....	3
	J. The Internal Control Unit (ICU).....	3
020.7	Specific Responsibilities for Special Operations Funds.....	4
	A. SOS Account Cashier	4
	B. The Disbursing Officer	4
	C. Accountable Officer.....	4
	D. Reporting Losses, Shortages, or Thefts.....	4
020.8	Allowable Expenditures	5
	A. Payment to Informants.....	5
	B. Supplies and Equipment	5
	C. Surveillance Expenses	5
	D. (b) (7)(E)	5
	E. (b) (7)(E)	5
	F. Emergency Expenditures	5
020.9	Unallowable Expenditures	6
020.10	Procedures for Establishing SOS Accounts.....	6
020.11	Procedures for Obtaining Funds.....	7
	A. SOS Accounts	7

B.	Special Operations Funds from OIG Headquarters	9
020.12	Procedures for Replenishments to SOS Accounts.....	12
020.13	Unannounced Cash Counts for SOS Account Funds	14
020.14	Procedures for Remittance of Funds Advanced by OIG Headquarters.....	14
A.	Sources of Funds.....	14
B.	Procedures for Remitting Operation Specific Funds	15
C.	Procedures for Remitting Funds as a Result of the Liquidation of an SOS Account	15
020.15	Recordkeeping Requirements	16
A.	SOS Accounts	17
B.	Special Operations Funding from Headquarters	18
020.16	Audit Responsibilities	19
A.	SOS Accounts	19
B.	Special Operations Funding from Headquarters	19
APPENDIX A	20
APPENDIX B	22

Table of Contents

022.1	Policy.....	1
022.2	Reference	1
022.3	Scope.....	1
022.4	Responsibilities.....	1
	A. All Approving Officials.....	1
	B. The Inspector General.....	1
	C. The DIG	2
	D. The AIG for Management and Planning	2
	E. AIGs and GC.....	2
	F. Additional Delegation to the AIG for Investigations.....	2
	G. Redelelegation of Authority.....	2
	H. Claimant.....	2
022.5	Procedures.....	3
	A. Authorized Uses.....	3
	B. Unauthorized Uses.....	5
	C. Corrections on Forms.....	6
	D. Reimbursement Procedures	6
022.6	Forms	7
APPENDIX A	7

Table of Contents

210.1	Purpose	1
210.2	Scope.....	1
210.3	Authority.....	1
210.4	Policy	1
210.5	Responsibilities.....	1
210.6	Actions Covered by the Merit Staffing Plan.....	3
210.7	Actions Not Covered by the Merit Staffing Plan.....	4
210.8	Area of Consideration	6
210.9	Vacancy Announcements.....	6
	A. Announcement Content	6
	B. Open Continuous Announcements	7
	C. Open Period.....	8
	D. Cancellation of Vacancy Announcements.....	8
210.10	Methods of Locating Candidates	8
	A. Noncompetitive Selections	8
	B. OIG Announcements	8
	C. Departmental Announcements	8
210.11	Application Procedures	8
	A. Withdrawal of Applications.....	9
	B. Applicant Notification	9
210.12	Candidate Evaluation Procedures	9
	A. Determining Basic Eligibility and Qualification Requirements	9
	B. Selective Placement Factors	9
	C. Other Eligibility Requirements.....	9
	D. Evaluation Criteria.....	9
	E. Evaluation and Ranking Procedures.....	10
	F. Numerical Rating.....	11
	G. Referral and Selection.....	12
	H. Release	12
	I. Notification to Individuals Selected and Entrance on Duty.....	13
	J. Additional Certification from Previous Vacancy Announcement.....	13
	K. Probationary Period.....	13
210.13	Employee Grievances and Corrective Actions	13
	A. Grievances.....	13

	B. Grievance Procedures	13
	C. Discrimination Complaints.....	13
	D. Action to Rectify Violations	13
	E. Corrective Action.....	14
210.14	Records to be Maintained, Information to be Made Available to Employees, and Agency Review.....	14
	A. Records to be Maintained	14
	B. Information to be Made Available.....	14
	C. Agency Review	15

Table of Contents

211.1	Policy	1
211.2	Reference	1
211.3	Scope.....	1
211.4	Responsibilities.....	1
	A. Employees	1
	B. Supervisors.....	1
	C. Management and Planning Division	1
	D. The Security Officer and the Designated Agency Ethics Officer	2
211.5	Procedures (Completion and Processing of Exit Clearance Form (V-211/1)).....	2
APPENDIX A.....		5

Table of Contents

235.1	Purpose	1
235.2	References	1
235.3	Definitions	1
	A. Mentor	1
	B. Mentee	1
235.4	Responsibilities	1
	A. Mentoring Program Coordinator	1
	B. Supervisors and Managers	2
	C. Mentors	2
	D. Mentees	3
235.5	Professional growth and development of employees	3
	A. Each mentee	3
	B. As deemed appropriate	3
	C. Pathways Program	3
	D. Other opportunities for the mentee	3
	E. Eligibility	4
	F. Requirements	4
	G. Selection of Mentoring Participants	4
	H. Selection of MP Participants	5
	I. Mentor Matches	5
	J. Program Commitments	6

Table of Contents

252.1	Purpose	1
252.2	Scope.....	1
252.3	Policy	1
252.4	Procedures and Responsibilities.....	1
	A. CASH	1
	B. Evaluators.....	1
	C. Panel	1
252.5	General.....	2
	A. Description	2
	B. Criteria.....	2
	C. Award	3
	D. Submission Procedures	3
	E. Documentation	3
	F. Inventions and Patent Disclosures.....	4
	G. Requests for Reconsideration	4
	APPENDIX A.....	6
	APPENDIX B.....	8

Table of Contents

260.1 Policy 1

260.2 References..... 1

260.3 Scope..... 1

260.4 Responsibilities..... 1

 A. Supervisors 1

 B. Employees..... 2

 C. Timekeepers..... 2

 D. Office of Human Resources..... 2

260.5 Basic Work Week 2

260.6 Lunch Period..... 3

260.7 Alternate Work Schedules. 3

 A. General..... 3

 B. Eligibility. 3

 C. Temporary Duty Assignments (TDY) and Training 3

260.8 Flexible Work Schedules 4

 A. The Flexitour Schedule..... 4

 B. The Gliding Schedule 4

 C. The Maxiflex 4

260.9 The Compressed Workweek Schedule (CWS)..... 6

 A. The CWS 5/4/9 schedule 6

 B. The CWS 4/10 schedule 7

260.10 Procedures..... 7

 A. Employee Request 7

 B. Basis for Disapproving or Cancelling an AWS Request..... 8

 C. Resolving Conflicts in AWS Requests..... 8

260.11 Leave..... 8

260.12 Holidays 8

 A. Maxiflex..... 9

 B. In Lieu of Holiday 9

 C. Holiday Worked..... 10

260.13 Credit Hours..... 10

 A. Eligibility 10

 B. Earning Credit Hours..... 10

	C.	Applying Credit Hours	10
	D.	Conversion to CWS	10
	E.	Carrying Over and Advancing Credit Hours	11
	F.	Exceptions to Earning Credit Hours	11
	G.	Other Considerations	11
	H.	Accountability.....	11
260.14		Overtime and Compensatory Time General	11
	A.	Eligibility	12
	B.	Special Situations.....	12
	C.	Responsibilities.....	12
	D.	Biweekly Cap on Premium Pay	12
	E.	Part-time Employees.....	13
260.15		Night Differential.....	13
	A.	Night Differential Payment.....	13
	B.	Pre-Approval of Night Differential Payment	13
		Appendix A.....	15
		Appendix B.....	17

Table of Contents

280.1	Policy.....	1
280.2	Reference.....	1
280.3	Scope	1
280.4	Responsibilities	1
280.5	Use and Misuse	2
280.6	Penalties for Misuse	2
	A. 18 U.S.C. 499	2
	B. 18 U.S.C. 506	2
	C. 18 U.S.C. 701	2
280.7	Credentials.....	2
	A. Eligibility.....	2
	B. Photographs	2
	C. Processing, Issuing, and Controlling Credentials.....	2
	D. Expiration Dates	3
	E. Credentials and Badges for Special Agents	3
280.8	OIG Identification Cards	3
280.9	Proximity Cards.....	3
	A. Eligibility.....	3
	B. Photographs	3
	C. Processing, Issuing, and Controlling Proximity Cards.....	3
280.10	PIV Cards	3
	A. Eligibility.....	4
	B. Photographs	4
	C. Processing, Issuing, and Controlling PIV Cards	4
	D. Expiration Dates	4
280.11	Courier Cards	4
280.12	Temporary Identification Cards	4
280.13	Replacement of Worn, Damaged, or Out-of-Date Identification Documents.....	4
280.14	Replacement of Expiring Identification Documents	5
280.15	Replacement of Credential Cases.....	5
280.16	Lost or Stolen Identification Documents.....	5
280.17	Termination of Employment	5
280.18	Retirement	6
	A. Retired Law Enforcement Badges for Special Agents.....	6
	B. Secondary Badges for Retired Special Agents.....	6
	C. Retiree ID Cards for Retired Special Agents	6
	D. Special Agents Retaining Permits to Carry Firearms.....	7

APPENDIX A, Credential Receipt Form 7

Table of Contents

290.1	Policy.....	1
290.2	Reference.....	1
290.3	Scope	1
290.4	Responsibilities	1
	A. The Inspector General	1
	B. The Deputy Inspector General	1
	C. The IG, General Counsel, Assistant Inspectors General, and Office Heads	1
	D. The Assistant Inspector General, Management and Planning.....	1
	E. The Human Resources Officer	2
	F. Supervisors	2
	G. Employees	2
290.5	Definitions.....	2
	A. Days.....	2
	B. Grievance Official	2
	C. Employee Representative	2
	D. Fact Finder.....	2
	E. Grievance	2
	F. Grievance File	3
	G. Office Heads.....	3
	H. Personal Relief	3
290.6	Right to Present a Grievance	3
290.7	Matters Excluded.....	3
290.8	Use of Official Time	4
290.9	Grievance Procedures.....	4
	A. Contents.....	4
	B. Advice	4
	C. Employee Representative	5
	D. Filing	5
	E. Grievance Process	5
	F. Confinement of the Grievance	5
	G. Selection of the Grievance Official	5
	H. Conduct of the Inquiry	6
	I. Action by the Grievance Official	6
	J. Rejection of a Grievance	6
	K. File and Notification.....	6
	L. Performance Rating Changes	6

Table of Contents

303.1 Policy 1

303.2 Reference 1

303.3 Scope 1

303.4 Responsibilities 1

 A. The Designated Accrediting Authority 1

 B. The Security Programs Manager 1

 C. The Information Systems Security Officer (ISSO) 2

 D. Assistant Inspector Generals 3

 E. System Administrators 3

 F. Supervisors 3

 G. Employees and contractors 3

303.5 Procedures 4

 A. Requirement for Processing All OIG and DOJ Data.. 4

 B. System Sensitivity Designations 4

 C. Network Accounts 4

 D. Personnel Security 4

 E. Training 5

 F. Network Security Protections 5

 F. Personally Identifiable Information (PII) 6

 G. Disposal 6

 H. Physical Protections and Labeling 7

 I. Hardware 7

 J. Backup Tapes 7

 K. Personally Owned Handheld Devices 8

 L. Wireless Handheld Devices 8

 M. Other Wireless Technologies 8

 N. External Media 8

 O. Media Reuse 8

303.6 Telework 8

 A. Workstation 8

 B. Classified Information 9

APPENDIX A 10

Table of Contents

304.1	Policy.....	1
304.2	Reference.....	1
304.3	Scope.....	1
304.4	Responsibilities.....	1
	A. IT Project Managers.....	1
	B. Chief Innovation Officer.....	1
	C. IT Project Sponsors.....	1
	D. M&P OIT.....	1
304.5	Definitions.....	2
	A. Project Management.....	2
	B. The Project Management Institute.....	2
	C. The Project Management Support.....	2
	D. A Project Request.....	2
	E. Project Charter.....	2
	F. Work Breakdown Structure.....	2
	G. A Project Schedule.....	2
	H. Project Scope.....	2
	I. A Change Request.....	2
	J. A Post-Project Evaluation.....	3
304.6	Procedures.....	3
	A. Initiating.....	3
	B. Planning.....	4
	C. Executing.....	4
	D. Monitoring & Controlling.....	4
	E. Closing.....	4
	APPENDIX A: OIG IT Project Management Methodology.....	5

Table of Contents

305.1	Policy	1
305.2	Reference.....	1
305.3	Scope	1
305.4	Responsibilities	1
	A. Front Office Administrative Staff	1
	B. Chief Innovation Officer	1
	C. Vendors	2
305.5	Definitions	2
	A. Commercial Off-the-shelf (COTS)	2
	B. Industry Engagement.....	2
305.6	Procedures	2
	A. Initial Request.....	2
	B. Planning.....	3
	C. Etiquette and Reporting.....	3
	D. Evaluation and Follow-up	3

Table of Contents

306.1	Policy.....	1
306.2	Reference.....	1
306.3	Scope	1
306.4	Responsibilities	1
	A. CINO	1
	B. M&P OIT	1
306.5	Procedures	1
APPENDIX A: OIT Pilot Study Template.....		5

Table of Contents

401.01	Policy.....	1
401.2	References.....	1
401.3	Scope.....	1
401.4	Responsibilities.....	2
	A. Property Management Officer (PMO)	2
	B. Accountable Property Officer (APO)	2
	C. Property Custodian (PC)	3
	D. Supervisors	4
	E. Employees	4
401.5	Definitions.....	5
	A. Accountable Property	5
	B. Property Management Officer (PMO)	5
	C. Accountable Property Officer	5
	D. Property Custodian (PC)	5
	E. Property Management Information System (PROMIS)	5
	F. Personal Property	5
	G. Acquire	7
	H. Dispose	7
	I. Loss	7
401.6	Appointments	7
	A. PMO	7
	B. APO	7
	C. PC	7
401.7	Procedures	7
	A. Determination of Need	7
	B. Procurement	8
	C. Receipt of Accountable Property	10
401.8	PROMIS	12
	A. PROMIS is an automated system	12
	B. PROMIS produces a set of standard reports	13
401.9	Inventories	13
	A. Records Inventory	13
	B. Physical Inventory	13
	C. Damaged, Missing, Lost, or Stolen Property	15
401.10	Disposition of Personal Property	16
	A. Reporting	16
	B. Processing	16

APPENDIX A	19
APPENDIX B	20

Table of Contents

420.1	Policy.....	1
	A. Records and Information Management Policy.....	1
	B. OIG RIM Program	1
420.2	Reference.....	2
420.3	Scope.....	2
420.4	Responsibilities.....	3
	A. Inspector General	3
	B. Deputy Inspector General, General Counsel, Assistant Inspectors General, Regional Audit Managers, Special Agents in Charge, Directors, and Other Managers and Supervisors.....	3
	C. OIG Records Manager.....	4
	D. Division Records Liaisons.....	5
	E. Records Management Points of Contact.....	5
	F. Director, Office of Information Technology.....	6
	G. Director, Office of Administrative Services and OIG Contracting Officers.....	6
	H. Employees and Contractors.....	6
420.5	Definitions	7
420.6	OIG RIM Procedures and Guidance	7
420.7	RIM Program Elements.....	7
420.8	Life Cycle Management	7
	A. Creation and Capture.....	7
	B. Management and Use	8
	C. Retention and Disposition.....	8
420.9	Safeguarding OIG Records.....	9
420.10	Storage.....	9
420.11	Vital Records	9
420.12	Classified Records.....	9
420.13	Training Program	10
420.14	Electronic RIM Program	10
420.15	Electronic Records in Databases and Systems.....	10

420.16	Electronic Mail	10
	A. General.....	10
	B. Retention of E-mail Records.....	10
	C. Subject to a Litigation Hold.....	10
420.17	Backup Tapes.....	11
	A. General.....	11
	B. Information on Backup Tapes.....	11
	C. Backup Tapes are for Disaster Recovery	11
420.18	Backup Tapes Subject to a Litigation Hold.....	11
420.19	Litigation Hold and Preservation Plans.....	11
420.20	Evaluation of the OIG RIM Program.....	11
APPENDIX A	13

- 001.1 Policy. The Inspector General Manual (IGM) is the authorized means to codify the policies and standards (hereafter called directives) governing the operation of the Office of the Inspector General (OIG).
- 001.2 Reference. This chapter is issued pursuant to 41 CFR § 202-9.103, which directs each agency to provide policy and procedural guidance through an established directives program.
- 001.3 Scope. Provisions of this chapter apply throughout the OIG.
- 001.4 Responsibilities. The directives management responsibilities of OIG officials are as follows:
- A. The Inspector General (IG) initiates policy development and approves all OIG policy documents prior to issuance through the IGM system.
 - B. The Deputy Inspector General (DIG) initiates policy development, decides unresolved policy issues among the Assistant Inspectors General, and submits policy documents to the IG for consideration.
 - C. Assistant Inspectors General (AIGs) initiate and prepare directives within their respective areas of program responsibility.
 - D. General Counsel (GC) reviews directives for legal sufficiency.
 - E. The Assistant Inspector General for Management and Planning (AIG, M&P), through the Directives Coordinator (DC), manages the directives program of the OIG, assures OIG compliance with the requirements of this chapter, and assures the dissemination of directives following approval by the IG.
 - F. Master Manual Holders (MMHs) may maintain and keep current a hard copy of all volumes of the IGM, as directed by the office head.
- 001.5 Manual Structure.
- A. Volumes. The IGM consists of five Volumes. They are: Volume I, Executive Direction; Volume II, Audit; Volume III, Investigations; Volume IV, Evaluation and Inspections; and Volume V, Management and Planning. The chapters included in the various volumes of the IGM are listed in a Master Table of Contents at the front of Volume I.
 - B. Number System. The IGM is divided into parts using the following system.

Volumes - I, II, III, IV, V

Chapters - 001 through 999
Subsections - A through Z
Paragraphs - (1), (2), (3), etc.
Subparagraphs - a, b, c, etc.

If a further subdivision is required, lower case Roman numerals (e.g., i, ii, iii, iv) may be used. A dash (-) symbol may be used if items listed do not require distinct identification.

- C. Table of Contents. A Master Table of Contents, which encompasses all five volumes of the IGM, is located at the front of Volume I. Each chapter with at least 5 pages has a Table of Contents at the beginning of the chapter. The DC will produce the Master and chapter Tables of Contents after all comments and revisions have been made.

001.6 Chapter Content.

- A. Required Sections. The following sections must appear in all OIG directives.

- (1) Policy. This section states the policies of the OIG that apply to the directive.
- (2) Reference. This section cites the underlying statutes and regulations that pertain to the issuance of the directive.
- (3) Scope. The scope will generally encompass the OIG workforce; however, it may be used to limit or define areas of application.
- (4) Procedures. This section contains the substantive body of the directive. Its precise nature, structure, and length will be determined by the needs of the subject being addressed.

- B. Optional Sections.

- (1) Responsibilities. This section immediately follows the Scope section and defines significant position-specific responsibilities.
- (2) Definitions. This section immediately follows the Responsibilities section. If the number of definitions required is large, include them in an Appendix, or for a large number of technical definitions, by reference to an appropriate GAO, OMB, Treasury, GSA, or OPM document, if available.
- (3) Reporting Requirements. Directives that involve reports or reporting requirements must contain a section explaining those requirements. This should be the last section in the directive.

- (4) **Forms.** Sample forms discussed in the directive, together with any additional instructions regarding their preparation, may be added as an appendix.

001.7 Procedures.

A. **Publication.** The IGM will be revised as needed. At the discretion of the IG, the IGM may be amended at any time.

B. **Preparation.**

- (1) **Responsibility for Preparation.** AIGs are responsible for the substantive content of draft directives in their division volumes. Chapter numbers for new directives should be obtained from the DC.
- (2) **Technical Requirements.** To promote a uniform and efficient IGM system, the technical requirements outlined in Appendix A must be met.

C. **Coordination.** The following system of coordination is prescribed to assure an adequate and timely consideration of management views within the OIG.

- (1) The originating AIG will forward draft directives via e-mail or on diskette to the DC.

Together, the originating AIG and the DC will identify the divisions impacted by the new directive. The DC will then forward the draft directive, using the Directives Review and Comments Form, OIG Form I-001/2 (11/23/05), (See Appendix C), to the AIGs of affected divisions and the GC.

- (2) Recipients will have 10 working days to comment and respond to the DC, unless a request for an extension has been made and granted by the DC. Nonresponse within the established time frame constitutes concurrence.
- (3) The DC will forward all comments to the originating AIG, who is responsible for incorporating any accepted changes, providing a written explanation for any excluded recommended changes, and forwarding the directive via e-mail or on diskette to the DC. In either case, the Directives Review and Comment form(s) will be a part of the package forwarded to the DC.
- (4) The DC will review the draft document within five working days to assure the draft is in compliance with the structural, content, and technical requirements of this chapter, and that appropriate officials had the opportunity to review the document.

The DC will incorporate any formatting changes and will submit the proposed directive to the DIG. As the originating AIG will have approved a draft directive before it is sent to the DC, formal concurrence from the originating AIG will not be sought during the review process.

The material submitted to the DIG will include:

- a. The Directives Review and Comment Forms that identify concurrences or nonconcurrences and which append any comments from nonconcurring officials.
- b. The directive, including an updated Master Table of Contents and Chapter table of contents (if appropriate) prepared by the DC.

The DIG will complete a review of the revised directive within 10 business days.

- (5) The DC will incorporate formatting or grammatical modifications made by the DIG. If the changes deal with policy issues, the DC will forward the package to the originator, who must resolve these issues with the DIG.
- (6) The DC will prepare a corrected version of the directive and submit it to the DIG.
- (7) The DIG will submit the proposal to the IG.

D. Approval. The IG has sole approval authority.

E. Dissemination. Following approval by the IG, the DC will promptly arrange for the new or revised directive(s) and the revised Master Table of Contents to be posted on the intranet and then notify the MMHs via e-mail that the new or revised directives(s) are available on the OIG intranet.

F. Circulation and Maintenance.

- (1) A Master Manual, consisting of all five volumes, may be maintained at divisional Headquarters and at each field installation.
- (2) An employee should be designated as the MMH. MMHs are responsible for keeping the IGM complete and current and for notifying employees in their respective offices whenever changes are made.
- (3) To assure adequate knowledge among the staff of OIG policies, standards, and procedures, MMHs should notify staff via e-mail of new releases on the intranet.

- (4) If hard copies are maintained, revised directives should replace older versions in the IGM. If MMHs or OIG employees wish to retain the older version behind the revised directive, the older version should be marked "canceled."

G. Revisions and Revalidation.

(1) Revisions.

- a. Revisions will be accomplished using the same methods as described in Section 001.7B through Section 001.7F, above.
- b. Revisions to the chapter will be detailed and explained in a separate document placed at the end of the chapter. Appendix B contains the format for detailing revisions.

(2) Revalidation. A biennial review will be made of each manual chapter to ascertain whether the chapter is still required and whether revisions are needed.

- a. The originating AIG of the division with substantive responsibility for a manual chapter will be notified by the DC 60 days prior to the expiration of the 2-year period. Nonresponse by the responsible AIG will result in the cancellation of the manual chapter after notification of the impending cancellation.
- b. The responsible AIG will determine whether revision and reissue is required, and if so, will process the revision by following the complete process set forth in this chapter.
- c. The IG has the discretion to require revalidation and revision at any time.

H. Interim Guidance. When it is necessary to issue memoranda that contain policy direction and instruction before a manual chapter can be developed or revised, the AIG may issue interim guidance pursuant to the following requirements.

(1) Format.

- a. Prepare in memorandum format.
- b. Print on blue paper to distinguish it from other written material/forms of documentation.

- c. Mark with a file reference from the IGM numbering system to facilitate uniform filing. The file reference should include the volume number, chapter number, and directive title. For example, interim guidance amending this directive would have the following file reference.

IGM Volume I, Chapter 001
"Directives Management System"

When using interim guidance to issue new policy not currently in the IGM, contact the DC for the volume and chapter number; divisions may determine chapter title. Under the file reference, type "New Directive."

(2) Distribution and Filing.

- a. The originating AIG will distribute electronic copies to the affected OIG offices, the General Counsel, the Immediate Office of the IG, and the DC.
 - b. MMHs may distribute copies internally according to distribution codes and may file interim guidance in the master IGM binders preceding the referenced chapter.
- (3) Incorporation into IGM. The originating AIG must develop new or revise an existing directive that incorporates the interim guidance. After the new or revised directive is issued and disseminated, interim guidance should be removed from all IGMs.

APPENDIX A

Technical Requirements

APPENDIX A

TECHNICAL REQUIREMENTS

- A. Software. All directives will be created in the standard OIG word processing software, MS Word. The font will be Times New Roman 12 point. The Management and Planning Division will provide the template to be used with complete instructions to each component as needed.
- B. Format and Style.
1. Page Headers. A standard page heading, similar to that used for this chapter, has been included on the formatted diskette and will be automatically produced for each page. Additionally, second and later pages of chapters will include at the top margin immediately below the standard heading a reference to the chapter, section, and if applicable, the subsections, paragraphs, and subparagraphs which apply to the first item discussed on the page, if the discussion continued from the previous page. This is not necessary when a new section begins at the top of a page.
 2. Page Footers. The DC will have completed the page footer as follows.
 - a. Distribution. The distribution code will be inserted at the left margin. The standard codes are:

A = Master Manual Holders	E = Support Personnel
B = Auditors	F = All Employees
C = Inspectors	G = Other (Specify
D = Investigators	
 - b. Draft directives. Until a directive has been approved for publishing, include the words "Revised (Draft)" centered on the Distribution line at the bottom of the page.
 - c. New directives. New directives approved for publishing include the words "NEW ISSUANCE" centered on the Distribution line at the bottom of the page.
 - d. Revised directive. Revised directives approved for publishing include the word "REVISED" centered on the Distribution line at the bottom of the page.
 - e. Page dating. The date of transmittal will appear in the lower right-hand corner of all pages.

3. Page numbering. Page numbers will be shown at the bottom middle of each page, in the area reserved for processing and distribution information. This has also been pre-set and will be automatically produced using the formatted diskette.
4. Justification and Hyphenation. Use left justification. Hyphenation is permitted, but not mandated.

APPENDIX B

Example of Revisions Page

APPENDIX B

Example:

INSPECTOR GENERAL MANUAL
Volume [I, II, III, IV, or V], Chapter [XXX]
[Title of Chapter]
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

List the pertinent sections that have been revised including changes, additions, and deletions. Use narrative to further explain, completely, any revisions.

001.1:

001.2:

001.3:

001.4:

001.4A:

001.6A(1):

001.6B(4):

And so on.

APPENDIX C

Directives Comments & Review Form
OIG Form I-001

INSPECTOR GENERAL MANUAL
Volume I, Chapter 001
Directives Management System
Revisions

This chapter was originally issued on November 23, 2005. It was revised on February 22, 2006 and February 5, 2018.

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

001.4E: The word “may” has been added reflecting that the MMHs do not have to keep the IGM in hard-copy form.

14 F: This is an addition. The General Counsel has the responsibility to ensure legal sufficiency.

15 A: The words “Evaluation and” have been added reflecting the correct title of the E&I division

001.7C(1): The form number “OIG Form I-001/2”, the date “(11/23/05)”, and “(See Appendix C) have been added.

001.7C(2): The words “for an extension” and “made” have been added to clarify the paragraph about the time period for responses.

001.7C(6): This is an addition. By adding this step in the process, any comments made by the DIG will be after the AIGs have made theirs. The DIG should be the final reviewer.

001.7E: This paragraph has been changed reflecting the policy of electronic availability and dissemination of the IGM.

001.7F (2, 3, and 4): These paragraphs have been changed reflecting the policy of electronic notification of changes to the IGM to staff by the MMHs.

001.7G(1)b: The policy on revisions to the IGM has changed. All substantive changes will be documented in a separate document following the last page of any chapter that has been revised.

001.7H(2)a: The originating AIG will be responsible for distributing “electronic” copies of the Interim Guidance.

001.7H(3): Added the words “should be removed” to the paragraph.

001.7G(2): Changed the required revalidation period from two years to five years, in order to better align with the DOJ Directive Management program.

- 002.1 **Policy.** The Inspector General (IG) and the Executive Staff of the Office of the Inspector General (OIG) will observe and clearly communicate the mission, organization, and functions of the OIG to their employees, the Department of Justice (DOJ), the Executive Branch, and Congress.
- 002.2 **Reference.** The Inspector General Act of 1978 (Public Law 95-452, October 12, 1978) as amended by the Inspector General Act Amendments of 1988 (Public Law 100-504, October 18, 1988); the Inspector General Reform Act of 2008 (Public Law 110-409, October 14, 2008); Attorney General (AG) Order 1941-89 (April 14, 1989); AG Order 1931-94 (November 8, 1994); and AG Order 2492-2001 (July 11, 2001).
- 002.3 **Scope.** This chapter applies throughout the OIG.
- 002.4 **Procedures.** Sections 002.5 through 002.7 describe the mission of the OIG and organizational structure and functions of the IG and Executive Staff.
- 002.5 **Mission Statement.** The OIG promotes integrity, accountability, efficiency, and effectiveness in the programs and operations of DOJ by the use and coordination of investigative, evaluation, inspection, and audit resources to:
- A. Investigate alleged violations of criminal and civil law, regulations, and ethical standards arising from the conduct of DOJ employees, contractors, and grantees, with the exception that allegations of misconduct by a Department attorney or law enforcement personnel that relate to the exercise of the Department attorney's authority to investigate, litigate or provide legal advice are the responsibility of the Department's Office of Professional Responsibility.
 - B. Conduct, report, and follow up on financial audits of DOJ organizations, programs, contracts, grants, and other agreements;
 - C. Conduct, report, and follow up on performance audits, evaluations, and inspections of programs and operations within or financed by DOJ; and
 - D. Report to the Attorney General and Congress on problems and deficiencies in the administration of DOJ and DOJ-financed programs and operations and on progress made in implementing recommended corrective actions.
- 002.6 **Organizational Structure.** The OIG includes an Immediate Office of the IG and five divisions: Audit, Investigations, Evaluation and Inspections, Oversight and Review, and Management and Planning. The Executive Staff consists of the IG, Deputy Inspector General (DIG), Senior Counsel, General Counsel, and an Assistant Inspector General for each of the five divisions. OIG organization charts are located on the OIG public website and on OIGNet.
- 002.7 **Function Statements.**
- A. **Inspector General.**
 - (1) Administers all functions assigned to the OIG by enabling legislation.
 - (2) Advises the Attorney General on fraud, waste, abuse, and integrity laws and policies.

- (3) Serves as a member of the Council of the Inspectors General on Integrity and Efficiency established by the Inspector General Reform Act of 2008.
- (4) Reports to the Attorney General and Congress regarding the status of completed audits, inspections, evaluations, investigations, and special reviews and on recommendations for corrective action and the progress made in implementing such actions.

B. Deputy Inspector General.

- (1) Administers the daily operations of the OIG.
- (2) Administers OIG policy and direction through the operational and executive staff.
- (3) Serves as the Acting Inspector General in the absence of the IG.
- (4) Advises the IG on all aspects of OIG activities and functions.
- (5) Serves as the action officer on programs, projects, or activities requiring executive direction and participation.

C. Senior Counsel.

- (1) Advises the IG on substantive and legal matters of concern to the OIG.
- (2) Provides advice and counsel on the formulation and implementation of OIG policies, procedures, and practices.
- (3) At the request of the IG, handles cases and oversees or coordinates special projects that require the attention of the IG's immediate staff.
- (4) Serves as a liaison to DOJ officials, other governmental officials, congressional staff, and the media as requested by the IG.
- (5) Acts as the IG's designated official to review information about complaints alleging abuses of civil rights and civil liberties by employees and officials of DOJ.

D. General Counsel.

- (1) Serves as the legal officer and advisor to the OIG. Participates in the formulation of policies and procedures for the OIG. Advises on the legal and policy consequences of proposed activities and programs. Manages litigation in which the OIG is involved.
- (2) Serves as the OIG's Deputy Designated Agency Ethics Official and manages the OIG ethics training and compliance program.
- (3) Manages the OIG Freedom of Information Act (FOIA) and Privacy Act (PA) program.
- (4) Serves as liaison with DOJ officials and legal staffs, as well as with officials and legal staffs in other government agencies.

- (5) Provides any certification required to authenticate books, records, and other documents as true copies of official OIG records.
- (6) Provides direction, guidance, and legal process as needed in the preparation of Inspector General subpoenas, other than routine requests for telephone records, and makes recommendations to the IG regarding the exercise of subpoena authority.
- (7) Provides legal advice and guidance to the Investigations Division on investigative issues.

E. Assistant Inspector General, Audit Division.

- (1) Advises the IG and the DIG on all matters pertaining to DOJ-wide audit policies, standards, and procedures.
- (2) Establishes and develops OIG audit policies, standards, and procedures.
- (3) Administers the programs and activities of the Audit Division and ensures the audit programs and activities conform to OIG and Government Accountability Office policies, standards, and procedures.
- (4) Conducts, reports, and follows up on internal audits of DOJ programs and activities, including the required annual financial statement audits of DOJ, and on external audits of DOJ's contracts, grants, or other agreements.
- (5) Develops and executes the OIG's audit work plan.

F. Assistant Inspector General, Investigations Division.

- (1) Advises the IG and the DIG on all matters pertaining to the detection, investigation, and prosecution of suspected violators of fraud, abuse, and integrity laws within DOJ.
- (2) Establishes and develops OIG investigative policies, standards, and procedures and recommends appropriate policies and directions.
- (3) Administers the programs and activities of the Investigations Division.
- (4) Administers the OIG Hotline. Reviews allegations and assigns for further investigation, or refers them to the appropriate DOJ component. Advises the IG of significant trends disclosed while operating the Hotline and maintains liaison with other Inspector General Hotlines for the referral of allegations, as appropriate.

G. Assistant Inspector General, Evaluation and Inspections Division.

- (1) Advises the IG and the DIG on all matters pertaining to DOJ-wide evaluation and inspection policies, standards, and procedures.
- (2) Establishes and develops OIG evaluation and inspection policies, standards, and procedures.

- (3) Administers the programs and activities of the Evaluation and Inspections Division.
- (4) Conducts, reports, and follows up on evaluations and inspections of DOJ programs and activities through methodologies such as program, operational, or follow-up reviews.

H. Assistant Inspector General, Oversight and Review Division.

- (1) Advises the IG and the DIG concerning allegations of criminal and noncriminal misconduct within the jurisdiction of the OIG.
- (2) Establishes and develops OIG policies, standards, and procedures regarding oversight and review matters.
- (3) At the request of the IG, handles complex, sensitive, or high-profile investigations or reviews of DOJ matters.
- (4) At the request of the IG, conducts compliance and quality reviews of OIG operations.
- (5) Conducts investigations of allegations of misconduct against OIG employees.
- (6) Administers the programs and activities of the Oversight and Review Division.

I. Assistant Inspector General, Management and Planning Division.

- (1) Advises the IG and the DIG on all matters pertaining to overall financial management, human resource management, security programs, equal employment opportunity, planning, information technology, contracting, procurement, property management, records management, internal controls, general administration, and other support services.
- (2) Establishes and develops OIG policy in all areas of operational and technical support, including administration, equal employment opportunity, information systems, personnel, security, records management, finance, contracting and procurement, internal controls, and long range planning.
- (3) Administers the programs and activities of the Management and Planning Division.
- (4) Serves as the Chief Financial Officer and the Chief Information Officer for the OIG.
- (5) Prepares the semiannual reports to the Attorney General and Congress.

Revisions

This chapter was originally issued on December 31, 1991, and was revised on October 10, 1996, and again on April 22, 2009.

002.5: Evaluations have been added to this section to further clarify the Mission Statement of the OIG.

002.5A: This section clarifies that complaints or allegations of misconduct by a Department attorney or law enforcement personnel and their ability to investigate, litigate, or provide legal advice are handled by the Department's Office of Responsibility, not the OIG.

002.6: This section has been changed to reflect the full name for the Evaluation and Inspections Division and to include the Oversight and Review Division. This section was also updated to reflect the current composition of the OIG Executive Staff. In addition, the position, Counselor to the IG, has been removed from this IGM chapter.

002.7A: This section removed a reference to the now defunct President's Council on Integrity and Efficiency.

002.7C: The duties of the Counselor to the IG and the Senior Counsel have been merged into a position called Senior Counsel. Deleted specific reference to providing oversight regarding the Federal Bureau of Investigation and the Drug Enforcement Administration.

002.7D(1): This section now includes the duty, Manages litigation in which the OIG is involved.

002.7D(2): This section now includes the duty, Serves as the OIG's Deputy Designated Agency Ethics Official and manages the OIG ethics training and compliance program.

002.7D(4): This section now includes the duty, Serves as liaison with DOJ officials and legal staffs, as well as, with officials and legal staffs in other government agencies.

002.7D(7): This section now includes the duty, Provides legal advice and guidance to the Investigations Division on investigative issues.

002.7F(4): This section has been changed to include responsibility of reviewing OIG Hotline allegations before assigning them for further investigation or referring them to the appropriate DOJ component.

002.7G: This section has been changed to include responsibility for evaluation policies, standards, and procedures.

002.7H(2): This section now includes the duty, Establishes and develops OIG policies, standards, procedures, regarding oversight and review matters.

002.7J: This section no longer includes the responsibility, Initiates or conducts special assignments, projects, investigations, or reviews for the IG, often in response to congressional or DOJ requests.

- 003.1 Policy. All delegations will be clearly stated in writing so there will be no doubt as to the authority and responsibilities of management and staff of the Office of the Inspector General (OIG).
- 003.2 Reference. The Inspector General Act of 1978 (Public Law 95-452, October 12, 1978) as amended by the Inspector General Act Amendments of 1988 (Public Law 100-504, October 18, 1988); the Inspector General Reform Act of 2008 (Public Law 110-409, October 14, 2008); and Attorney General Order No. 1341-1989, Delegating Certain Authorities to the Inspector General, Department of Justice (April 14, 1989).
- 003.3 Scope. This chapter applies throughout the OIG.
- 003.4 Procedures. Sections 003.5 through 003.15 outline the authorities retained by the Inspector General and authorities delegated to Executive Staff within the OIG. Overall management delegations are included in this chapter, and overall administrative and operational delegations are found in appropriate subject matter chapters.
- 003.5 Authorities Retained by the Inspector General (IG). Authorities not specifically delegated in this chapter or elsewhere in the Inspector General Manual (IGM) are retained by the IG. The IG retains the following authorities and activities.
- A. Promulgation of all policy issuances and approval of all materials to be included in the IGM.
 - B. Approval of all major plans of the OIG, including but not limited to:
 - (1) The Annual Audit Plan and all revisions thereto.
 - (2) Evaluation plans and all major revisions to the scope of reviews.
 - (3) The Annual Budget submission and all supplemental requests.
 - (4) All reorganizations of components of the OIG.
 - (5) The OIG Strategic Plan.
 - C. All contacts with the Attorney General or the Deputy Attorney General.
 - D. All contacts with the Director or Deputy Director of the Office of Management and Budget.
 - E. All contacts, above the staff level, with the Congress.
 - F. All contacts with the Controller General of the United States and the Inspectors General of other departments. Other members of the Executive Staff (as defined in the Inspector General Manual, Volume I, Chapter 002, Mission, Organization, and Functions), and

division staff as necessary to perform their duties, are authorized to deal with subordinate levels in the Government Accountability Office and other Inspector General offices, as appropriate.

- G. Representation on the Council of Inspectors General for Integrity and Efficiency (CIGIE). Contacts may be made by the Executive Staff on policy and administrative matters, as appropriate; however, the IG shall be informed about these contacts. OIG staff may engage in the contacts necessary to effectively pursue joint projects being conducted with the CIGIE, its staff, or subcommittees.
- H. All contacts with Department component heads on policy matters. The Executive Staff are authorized to deal with the components on administrative and operational matters.
- I. All contacts with the media not delegated in Volume I, Chapter 032, OIG Public Affairs; and Volume III, Chapter 032, Media Relations.

003.6 Delegation to the Deputy Inspector General (DIG).

- A. The DIG serves as Acting Inspector General in the IG's absence.
- B. The DIG, when acting on behalf of the IG, may exercise the full range of authority of the IG, subject only to the specific restriction of the IG.
- C. Subject to the general direction of the IG, the DIG shall be notified of the use of all non-routine investigative techniques conducted by employees of OIG. The DIG shall be notified in advance of:
 - (1) All undercover operations subject to the review of the CIGIE (or FBI) Undercover Review Committee as addressed in IGM Volume III, Chapter 250;
 - (2) All special fiscal circumstances related to undercover operations as addressed in IGM Volume III, Chapter 250, Undercover Operations Guidelines;
 - (3) All circumstances where the use of a non-routine investigative technique might result in significant publicity to the office.

003.7 Delegation to the General Counsel (GC).

- A. The GC is authorized to direct the GC activities as set forth in the approved functional statements in the IGM, Volume I, Chapter 002, Mission Organization, and Functions.
- B. The GC may exercise signatory authority in responding to Freedom of Information Act and Privacy Act requests.

- C. In the IG’s absence, the GC may exercise signatory authority of IG subpoenas that would otherwise require IG approval.

003.8 Delegation to the Assistant Inspector General, Audit Division (AIG/A).

- A. The AIG/A is authorized to direct the audit activities of the OIG as set forth in the approved functional statements in the IGM, Volume I, Chapter 002, Mission Organization, and Functions.
- B. The AIG/A may exercise signatory authority on audit-related documents, except the following documents which will require the approval of the IG.
 - (1) Those set forth in Section 003.5 of this chapter.
 - (2) Final internal audit reports.

003.9 Delegation to the Assistant Inspector General, Investigations Division (AIG/INV).

- A. The AIG/INV is authorized to direct the investigative activities of the OIG as set forth in the approved functional statements in the IGM, Volume I, Chapter 002, Mission Organization, and Functions.
- B. The AIG/INV may exercise signatory authority on investigation-related documents, except for those set forth in Section 003.5 of this chapter, which require the approval of the IG.

003.10 Delegation to the Assistant Inspector General, Evaluation and Inspections Division (AIG/E&I).

- A. The AIG/E&I is authorized to direct the evaluation activities of the OIG as set forth in the approved functional statements in the IGM, Volume I, Chapter 002, Mission Organization, and Functions.
- B. The AIG/E&I may exercise signatory authority on evaluation-related documents, except the following documents which will require the approval of the IG.
 - (1) Those set forth in Section 003.5 of this chapter.
 - (2) Initiation memoranda for evaluation and inspection reviews.
 - (3) Final evaluation and inspection reports.

003.11 Delegation to the Assistant Inspector General, Oversight and Review Division (AIG/O&R).

- A. The AIG/O&R is authorized to direct the oversight and review activities of the OIG as set forth in the approved functional statements in the IGM, Volume I, Chapter 002, Mission Organization, and Functions.

- B. The AIG/O&R may exercise signatory authority on oversight and review-related documents, except the following documents which will require the approval of the IG.
 - (1) Those set forth in Section 003.5 of this chapter.
 - (2) Final Oversight and Review Division reports.
 - (3) Initiation memoranda for Oversight and Review Division reviews.

003.12 Delegation to the Assistant Inspector General, Management and Planning Division (AIG/M&P).

- A. The AIG/M&P is authorized to direct the administrative management and planning activities of the OIG as set forth in the approved functional statements in the IGM, Volume I, Chapter 002, Mission Organization, and Functions.
- B. The AIG/M&P may exercise signatory authority on administrative and security-related documents, except those set forth in Section 003.5 of this chapter or otherwise restricted by the IG.

003.13 Delegation to the Contracting Officer (CO).

- A. The CO is delegated operational authority to oversee the contracting activity of the OIG.
- B. The CO may exercise signatory authority on documents relating to purchase orders and contracts, except those set forth in Section 003.5 of this chapter or otherwise restricted by the IG.
- C. The CO is delegated authority to ratify unauthorized commitments by non-procurement officials, provided that the following conditions are met:
 - (1) Supplies or services have been provided to and accepted by the Government, or the Government otherwise has obtained or will obtain a benefit resulting from performance of the unauthorized commitment;
 - (2) The resulting contract would otherwise have been proper if made by an appropriate CO;
 - (3) The CO reviewing the unauthorized commitment determines the price to be fair and reasonable;
 - (4) Funds are available and were available at the time the unauthorized commitment was made; and
 - (5) The ratification is in accordance with any other limitations prescribed under agency procedures.

- 003.14 Redelegation of Authority. The authorities delegated in this chapter may be redelegated to subordinate headquarters or field officials, as appropriate. All such redelegations shall be specified in an appropriate subject matter chapter of the IGM, as approved by the IG.
- 003.15 Continuity of Operations. In the event of the simultaneous absence of the IG and the DIG from the office, the IG or the DIG, acting in the IG's behalf, will designate in writing an Acting IG from among the Executive Staff.

INSPECTOR GENERAL MANUAL
Volume I, Chapter 003
Delegation of Authorities
Revisions

Throughout the chapter: Updated names of organizations and titles of IGM chapters, as necessary. Deleted references to and discussion of a former OIG unit, the Special Investigations and Review Unit.

003.2: Updated the reference section to include the Inspector General Reform Act of 2008 (Public Law 110-409, October 14, 2008); and the specific name and correct citation of Attorney General Order No. 1341-1989.

003.5.B(2): Expanded the extent of the IG's approval of evaluation plans.

003.5.B(5): Added the OIG Strategic Plan.

003.5D: Clarified the level of authorized contact between OIG personnel and the Office of Management and Budget.

003.6C: Updated the descriptions of the circumstances under which the DOJ must be notified in advance of certain investigative operations.

003.7.C: Added language regarding the General Counsel's authority to sign IG subpoenas in the IG's absence.

003.8 – 003.12: Re-ordered Sections to follow the order in IGM, Volume II, Chapter 002, Mission, Organization, and Function.

003.9: Deleted the AIG/INV's exercise of signatory authority for notifications to Heads of Department components regarding the results of investigations where the allegations have been substantiated.

003.9B: To clarify, deleted reference to the DIG at the end of the phrase "except for those set forth in Section 003.5 of this chapter, which require the approval of the IG."

003.10B(2): Deleted specific reference to "internal" reviews.

003.10B(3): Changed "work products" to "reviews."

003.11: Added a new section addressing the delegations of authority to the Assistant Inspector General of the Oversight and Review Division.

003.13: Added language regarding the delegation of the authority to ratify unauthorized commitments.

003.14: Edited language to specify that any redelegations of authority must be incorporated into the appropriate subject-matter chapters in the IGM, rather than in the appendices to this IGM chapter.

Appendices: Deleted the appendices that specified the delegations of authority by Assistant Inspectors General to others within their divisions.

- 021.1 Policy. This chapter establishes Office of the Inspector General (OIG) policy on the handling, appearance, and written style of official OIG correspondence, including memoranda, letters, and scheduling requests for the Attorney General (AG) and Deputy Attorney General (DAG). All official correspondence will be prepared in accordance with this directive.
- 021.2 Reference.
- A. OIG Correspondence Handbook.
 - B. OIG Editorial Style Guide.
 - C. Government Printing Office (GPO) Style Manual.
- 021.3 Scope. Provisions of this chapter apply throughout the OIG.
- 021.4 Responsibilities.
- A. The Inspector General (IG) and Deputy Inspector General (DIG) are responsible for:
 - (1) ensuring effective control, coordination, and timely processing of controlled correspondence;
 - (2) designating an employee to maintain liaison with those who submitted the correspondence;
 - (3) assigning the correspondence to a division or office when necessary;
 - (4) reviewing the draft response to the correspondence; and
 - (5) signing the official response.
 - B. The Executive Support Specialists to the IG, DIG, or Front Office Staff are responsible for:
 - (1) controlling all incoming correspondence addressed to the IG;
 - (2) reviewing the correspondence and establishing a process for completion;
 - (3) assigning action to the appropriate division or office;
 - (4) entering the correspondence in the correct tracking database, based on whether the correspondence came from Congress or another entity;
 - (5) establishing a process to ensure that due dates are met;
 - (6) notifying those who submitted the correspondence if an extension is needed;

- (7) coordinating with other divisions or offices that have an interest in the subject matter;
 - (8) reviewing correspondence documents for correct grammar and form;
 - (9) reviewing response drafts and preparing the final version for the IG's or DIG's signature;
 - (10) sending out the written response to the correspondence; and
 - (11) providing information copies to other interested parties.
- C. Assistant Inspectors General, Deputy Assistant Inspectors General, Regional Audit Managers, Assistant Regional Audit Managers, Special Agents in Charge, and Assistant Special Agents in Charge are responsible for:
- (1) submitting all controlled correspondence by the required due date established by the Immediate Office;
 - (2) ensuring that an extension is requested from the Immediate Office if for some reason the office cannot meet the due date, understanding that extensions may not be granted on certain congressional correspondence controlled by the Executive Secretariat; and
 - (3) ensuring that processes are in place to assure that all correspondence originated by the office is grammatically correct and in accordance with established policies and procedures before such documents are submitted for signature or concurrence.
- D. Office Managers for Assistant Inspectors General, Deputy Assistant Inspectors General, Regional Audit Managers, Assistant Regional Audit Managers, Special Agents in Charge, or Assistant Special Agents in Charge; Clerks, or other staff are responsible for:
- (1) preparing or reviewing correspondence documents in accordance with instructions in this directive; and
 - (2) ensuring that Office Managers maintain official files for correspondence that originates in their offices.
- E. OIG Personnel Who Initiate Correspondence are responsible for:
- (1) ensuring that the correspondence that they initiate meets applicable requirements referenced in this policy. Although OIG Executive Support Specialists usually

prepare and assemble correspondence packages, staff members should not rely exclusively on Executive Support Specialists for these functions. Personnel may be tasked to prepare correspondence and review documents for content, grammar, and form, as required;

- (2) following the appropriate process and preparation guidance outlined in the OIG Correspondence Handbook for controlled correspondence from the Immediate Office, congressional correspondence, and general correspondence;
- (3) following the guidance on style, grammar, and usage that is found in the OIG Editorial Style Guide, and Government Printing Office (GPO) Style Manual; and
- (4) consulting the Executive Secretariat Correspondence Manual for Attorney General correspondence.

021.5 Procedures.

- A. All Official Correspondence. All official correspondence addressed to recipients outside of the OIG must follow the processes and standards described in the OIG Correspondence Handbook, found on OIGNet under *OIG Style Standards*.
- B. Correspondence Not Controlled by the Immediate Office. The IG or the Immediate Office staff receives incoming correspondence that does not require a written response. The Immediate Office does not control this type of correspondence but forwards it to the appropriate Immediate Office staff or OIG office/division for action.
- C. Correspondence Controlled by the Immediate Office. The IG or the Immediate Office staff receives incoming correspondence that requires a written response. The Immediate Office controls the correspondence by tasking the response to the appropriate Immediate Office staff or OIG office/division along with an assigned due date. The Immediate Office then tracks the progress of the response, review, and distribution until the task is complete.
- D. Congressional Correspondence. If a division receives a congressional correspondence directly, the division shall forward the original incoming document(s) to the Immediate Office. The Immediate Office then determines if the congressional correspondence should be controlled and assigned.
- E. AG/DAG Scheduling Requests. When the IG or DIG desires that the AG or DAG attend a particular meeting or event, they direct the Executive Specialist to prepare an official scheduling request, according to the process outlined in the OIG Correspondence Handbook.

Revisions

This chapter was originally issued on December 13, 1991, and revised on June 19, 2012. This chapter has been reorganized and rewritten to reflect current guidance and use of technology.

Format: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

Throughout the Chapter: Details concerning process and formatting (for example, sections concerning administrative features, letter style correspondence, and memorandum style correspondence were extracted and placed into the OIG Correspondence Handbook.)

Throughout the Chapter: Details concerning writing style (including a dedicated section and Appendix F on writing, grammar, and usage) were omitted since the OIG now uses the OIG Editorial Style Guide and the Government Printing Office Style Guide for writing style guidance.

The section concerning congressional responses has been revised to indicate that congressional mail is not handled automatically as controlled correspondence.

The section and appendix (Appendix C) regarding Attorney General/Deputy Attorney General Action Memoranda was omitted because the OIG does not generate documents for the Attorney General/Deputy Attorney General's signature.

A section concerning Attorney General/Deputy Attorney General Scheduling Requests was added.

Appendices A, B, and B1 have become part of the OIG Correspondence Handbook.

- 030.1 **Policy.** Personnel are to be informed of the standards of conduct expected of them as employees of the Office of the Inspector General (OIG) of the Department of Justice (DOJ) and the reporting requirements relating to those standards.
- 030.2 **Reference.** This chapter is issued pursuant to:
- A. Title 18 U.S.C., Crimes and Criminal Procedure;
 - B. 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees in the Executive Branch;
 - C. 28 C.F.R. Part 45, Judicial Administration, Department of Justice, Employee Responsibilities;
 - D. Executive Order Number 12674 as amended by Executive Order No. 12731, "Principles of Ethical Conduct for Government Officers and Employees;"
 - E. Inspector General Act of 1978 as amended; and
 - G. Inspector General Reform Act of 2008.
- 030.3 **Scope.** Provisions of this chapter apply to all OIG employees, including any employees temporarily assigned to the OIG.
- 030.4 **Responsibilities.**
- A. **Employees.** It is the responsibility of each employee of the OIG to:
 - (1) know and observe the OIG Standards of Conduct and the laws and regulations governing federal and DOJ employee activities;
 - (2) secure proper approval for outside employment as required by the OIG Standards of Conduct;
 - (3) file any and all statements and reports required by the OIG;
 - (4) consult their supervisor or the Office of General Counsel (OGC) about any provision of the OIG Standards of Conduct;
 - (5) maintain the highest standards of honesty, integrity, and impartiality in their conduct and encourage others to do so; and
 - (6) advise their supervisor or OGC of any activity by an employee of the OIG that appears to violate the OIG Standards of Conduct or the regulations applicable to employment in the OIG, DOJ, or the federal government.
 - B. **Supervisors.** It is the responsibility of OIG supervisors to:
 - (1) set and maintain high standards of personal conduct as an example to employees;
 - (2) be aware of and apply fairly and impartially the OIG Standards of Conduct;

- (3) ensure that all present employees in their area of responsibility and candidates for employment within the OIG are informed of the OIG reporting requirements and Standards of Conduct, and that a copy of the current OIG standards as well as 28 C.F.R. Part 45 are maintained and made available to employees;
 - (4) report employee violations of the OIG Standards of Conduct and the laws and regulations governing federal and DOJ employee activities through their chain of command to the Inspector General (IG);
 - (5) ensure that employee requests to engage in outside employment are expeditiously considered and forwarded for appropriate consideration; and
 - (6) transmit any report made by an employee pursuant to § 030.7 of this chapter through their chain of command to the IG.
- C. The Oversight and Review Division. At the direction of the IG, the Oversight and Review Division will review and investigate alleged violations of this chapter, including reports made by an employee pursuant to § 030.7 below.
- D. The Office of General Counsel. It is the responsibility of the OGC to:
- (1) provide legal advice, guidance, and assistance with respect to the interpretation of matters relating to this chapter; and
 - (2) give prompt consideration to employee requests for outside employment.
- E. The Deputy Inspector General. It is the responsibility of the Deputy Inspector General (DIG) to hear appeals by employees of the denial of their requests for outside employment or the revocation of such approval.

030.5 Procedures.

A. Standards of Conduct.

- (1) OIG employees shall conduct themselves in a manner that creates and maintains respect for the OIG, DOJ, and the federal government. In their official and personal activities, they should remain mindful that, as employees of the OIG, they are expected to maintain the highest standards of behavior.
- (2) OIG employees are prohibited from engaging in any unethical, criminal, dishonest, or other conduct prejudicial to the OIG, DOJ, or the federal government.
- (3) In carrying out their official duties, OIG employees may not discriminate on the basis of race, color, religion, national origin, sex, gender identity, age, disability (physical or mental), genetic information, status as a parent, sexual orientation, marital status, political affiliation, or any other non-merit factor.
- (4) OIG employees shall not engage in any behavior that creates an intimidating, hostile, or offensive work environment. OIG employees should not make

unwelcome sexual advances on or request sexual favors from OIG employees or others encountered in the performance of OIG duties or engage in other verbal or physical harassment on the basis of race, color, religion, national origin, sex, gender identity, age, disability (physical or mental), genetic information, status as a parent, sexual orientation, marital status, political affiliation, or any other non-merit factor. OIG employees also should be sensitive to other OIG employees' sense of privacy, particularly in relation to social media. For example, OIG employees should not take photographs of other OIG employees in the workplace without their consent or post such photographs on social media sites without their consent.

- (5) Conflicts of interest may arise when there is a consensual romantic or sexual relationship between a supervisory employee and a subordinate employee. To avoid such potential conflicts or the appearance thereof and allegations of preferential or unfair treatment, a supervisory employee who becomes involved in a consensual romantic or sexual relationship with a subordinate employee must take actions to immediately cease serving as the subordinate employee's supervisor. The supervisory employee shall immediately notify his or her supervisor, or the OIG's Director of Office of Human Resources, of the relationship so that alternative arrangements can be made for the supervision of the subordinate employee. The supervisory employee shall not be involved, directly or indirectly, in decisions relating to salary, promotion, performance appraisals, work assignments, or other working conditions for a subordinate employee with whom such a relationship exists or existed. The subordinate's assignments and responsibilities shall not be negatively affected by changes to his or her supervision. The supervisory employee shall not recommend or serve as a reference for the former subordinate employee for a position within the OIG unless the supervisory employee discloses the existence of the ongoing or prior relationship with the former subordinate employee, and the supervisory employee shall not provide an official recommendation for the former subordinate employee to other prospective employers without disclosing the relationship. A supervisory employee's failure to comply with the requirements of this standard is a ground for disciplinary action.
- (6) Conflicts of interest and allegations of preferential or unfair treatment may arise when a supervisory employee has an outside financial or business relationship with a subordinate employee. Supervisory employees shall not engage in such relationships with their subordinates. A supervisory employee's failure to comply with the requirements of this standard is a ground for disciplinary action.
- (7) Supervisors are held to a higher standard than their subordinates regarding the responsibility to avoid conflicts of interest, the appearance of conflicts of interest, preferential treatment and the appearance thereof, and engaging in inappropriate conduct in connection with their supervisory duties. Therefore, supervisors may be subject to more serious discipline than their subordinates for non-compliance with these standards.
- (8) Except as part of an officially sanctioned internal investigation, an OIG employee may not record in any way a conversation with another OIG employee without the other employee's knowledge and consent.

- (9) OIG employees are prohibited from engaging in any outside employment without the express written approval of the OIG as provided in this chapter.
- (10) These standards of conduct and reporting requirements supplement those that apply to all federal employees as set forth in 5 C.F.R. Part 2635 and Title 18 U.S.C. and those that apply to DOJ employees as set forth in 28 C.F.R. Part 45, each of which is incorporated in this chapter by reference. Employees must also comply with requirements that appear elsewhere in the Inspector General Manual. The absence of a specific regulation covering conduct that brings discredit to or would be prejudicial to the OIG does not mean that such an act is condoned, permissible, or will not result in disciplinary or adverse personnel action.
- (11) An employee who engages in illegal activity, activity that may bring discredit to or would be prejudicial to the OIG, DOJ, or the federal government, or activity that creates a conflict of interest or otherwise violates the provisions of this chapter will be subject to disciplinary action, including, in appropriate circumstances, removal from federal service.
- (12) OIG employees receive and have access to sensitive information and documents provided to the OIG in the course of audits, evaluations, reviews, and investigations. An employee may not take non-public work products, documents, records, information, or other materials received from DOJ components or other agencies in the course of the employee's work for personal use at any time, including at time of separation from the OIG. All such non-public material, including non-public work product is property of the OIG and subject to DOJ Order 2710.8C, Removal and Maintenance of, and Access to, Documents.

- B. Outside Employment. An employee of the OIG is prohibited from engaging in any outside employment without the express written approval of the OIG in accordance with the terms of these standards.

Under no circumstances shall an OIG employee engage in any outside employment that will create or appear to create a conflict of interest, reflect adversely upon the OIG, DOJ, or federal government, in any manner interfere with their availability or the proper and effective performance of the duties of their position, or violate the OIG Standards of Conduct, the laws of the United States, or the regulations governing federal and DOJ employee activities.

(1) Definitions.

- a. The term *outside employment* means any type of employment exclusive of OIG employment, including self-employment, employment by a third party, or participation in any business or other entity, whether or not there is any compensation or profit to the employee. Self-employment includes any participatory interest in a business, corporation, or franchise.

Outside employment includes all teaching, speaking, or writing, whether or not the activity is compensated. If the outside employment

is approved, an employee may receive compensation for teaching, speaking, or writing as long as that activity is unrelated to an employee's official duties. Generally, teaching, speaking, or writing relates to an employee's official duties if:

- i. the activity is undertaken as part of the employee's official duties;
- ii. circumstances indicate that the invitation to engage in the activity was extended to the employee because of the employee's official position rather than the employee's expertise in the subject matter;
- iii. the invitation to engage in the activity or offer of compensation for the activity was extended by a person who has interests that may be affected substantially by the performance or nonperformance of the employee's official duties; or
- iv. the information conveyed through the activity draws substantially on ideas or official data that are nonpublic information; these provisions do not prohibit an employee from receiving compensation for teaching, speaking, or writing on a subject within the employee's discipline or inherent area of expertise based on the employee's educational background or experience, even though the teaching, speaking, or writing deals generally with a subject within the OIG's areas of responsibility.

Further guidance on teaching, speaking, or writing may be found at 5 C.F.R. 2635.807.

- b. The following endeavors are not considered outside employment for purposes of this standard and do not require prior OIG approval or notification. Employees engaging in such activity may not use government time, equipment, supplies, or funds in furtherance of such endeavors:
 - i. unpaid participation in and fund raising for youth, religious, educational (including parent-teacher associations), fraternal, community, or veteran activities that do not conflict with the OIG Standards of Conduct or the regulations applicable to employment in the OIG, DOJ, or the federal government;
 - ii. participation in the Military Reserves or National Guard;
 - iii. the ownership of investment instruments such as stocks and

bonds and an employee's personal management of investments owned by the employee or a member of the employee's family; and

- iv. the ownership of income-producing real estate. Management of real estate owned by third parties other than members of the employee's family, however, is considered outside employment including any employment as a "resident manager" of an apartment building or complex, even though the only pay received is in the form of reduced personal rent for the employee).

(2) Criminal Investigators - 1811 Series. Criminal investigators occupy positions that place a high premium on their time and attention. They are subject to being called to duty 24 hours a day. Outside employment by criminal investigators is prohibited, except that, subject to prior approval of the OIG as set forth below, criminal investigators may:

- a. engage in teaching, speaking, or writing; and
- b. receive compensation for recreational or hobby activities which have not been formally or informally contracted for in advance (e.g., a criminal investigator who enjoys woodworking may sell his work at a flea market but not fulfill special orders, or a criminal investigator who plays the piano may not accept payment as a piano teacher for a regularly scheduled class or lesson).

(3) Employees Other Than Criminal Investigators. OIG employees, other than criminal investigators, may engage in certain outside employment subject to the prior approval of the OIG as set forth below.

(4) Request and Authorization for Outside Employment - Right of Appeal. To obtain prior approval for outside employment, an employee must present OIG Form I-030/1, Request for Permission to Engage in Outside Employment, to their office head. (See Appendix A and see OIGNet for an electronic version of this form.) The office head will note their recommendation on the form and will forward it to the appropriate Assistant Inspector General (AIG) for approval. Upon approval by the AIG, the form will be forwarded to the OGC for final approval. The employee and the head of the office in which they work will be promptly advised of the disposition of the employee's request.

An employee whose request for approval for participation in outside employment has been denied by the cognizant AIG or the OGC may appeal such denial to the DIG. Such appeal must be in writing and must be submitted to the DIG within 30 days of the date on which the employee was advised of the action on their request. The employee shall be advised in writing of the disposition of the appeal.

- (5) Annual Renewal of Approval, Changes in Outside Employment. Employees who maintain outside employment in the same or similar capacity as previously approved must submit a new request for approval on OIG Form I-030/1 before January 31 of each year. Changes in outside employment, including new employment or changes in the duties and responsibilities in previously approved outside employment, must be approved before such change takes effect. Employees will be promptly advised of the disposition of their requests for approval.
- (6) Distribution of Approved Requests Copies of requests for outside employment that are approved will be distributed as follows:
 - a. original retained by the OGC for information and statistical purposes;
 - b. copy retained by the Office of Human Resources;
 - c. copy returned to employee; and
 - d. copy returned to employee's office head.
- (7) Use of Government Funds and Equipment. Employees who have secured approval to engage in outside employment other than teaching, speaking, or writing may not use government time, equipment, supplies, or funds in furtherance of that employment. Employees who have secured approval to engage in teaching, speaking, or writing must comply with DOJ regulations that allow personal use of government property only when such use involves negligible expense to the government. (See 28 C.F.R. 45.4).
- (8) Revocation of OIG Approval for Outside Employment. The cognizant AIG or the OGC may revoke an employee's previously approved participation in outside employment when continued participation is deemed to create or appear to create a conflict of interest, reflect adversely upon the OIG or DOJ, in any manner interfere with availability or the proper and effective performance of the duties of the employee's position, or violate OIG Standards of Conduct, the laws of the United States, or the regulations governing OIG, federal, and DOJ employee activities. Revocation of an employee's previously approved participation in outside employment shall be effective upon written notice to the employee. A copy of such notice shall be maintained by the employee's office head, the Office of Human Resources, and the OGC.

An employee whose approval for participation in outside employment has been revoked may appeal to the DIG. Such an appeal must be in writing and must be submitted to the DIG within 30 days of the date on which the employee was advised of such revocation. The employee shall be advised in writing of the disposition of the appeal.

030.6 Reporting Requirements.

- A. Occurrences an Employee Must Report. An employee must report in writing to their supervisor or a higher level official in the chain of command, and the OIG's Security Programs Manager the following occurrences. Such instances must be reported as soon as possible, but no later than three days, after their occurrence.
- (1) Any arrest or any instance in which the employee has been taken into custody, held for investigation, or detained for questioning, regardless of whether the employee was in a duty or non-duty status at the time of the occurrence.
 - (2) Any civil lawsuit or administrative complaint involving allegations that the employee engaged in a breach of professional standards, a breach of a fiduciary duty, or a claim for past due debt in an amount in excess of \$500.00.
 - (3) Citations for traffic violations while operating a personal vehicle need not be reported; however, any infraction resulting in arrest involving an official government vehicle (including a vehicle rented for official use) must be reported immediately.
- B. Actual or Potential Conflicts of Interest. An employee must report to their supervisor any actual or potential personal or financial conflict of interest.

Generally, a conflict of interest arises when an employee's official actions affect or appear to affect the personal or financial interest of the employee or a member of the employee's family.

A personal conflict of interest includes, but is not limited to, a personal or familial relationship with an individual doing business with the OIG or DOJ; an individual who is the subject of an OIG investigation; or an individual employed by an entity that is doing business with the OIG or is the subject of an OIG investigation, audit, evaluation, or review.

A financial conflict of interest may include, but is not limited to, a business relationship; discussions regarding future employment; payment for past services or employment; the ownership of stocks or bonds; service as a trustee, officer, or director; or the promise or receipt of something of value such as a loan or gift on the part of the employee or a member of the employee's family.

An employee should report to their supervisor any actual or potential conflict of interest as soon as the employee becomes aware of such conflict so that a determination can be made with regard to the continued assignment of any matter affected by that conflict, and any possible violation of the OIG Standards of Conduct, the laws of the United States, or the regulations governing the OIG and DOJ. Possible violations of the OIG Standards of Conduct, the laws of the United States, or DOJ regulations should be reported by the supervisor to the OIG and, through the supervisor's chain of command, to the IG.

U.S. Department of Justice
Office of the Inspector General

REQUEST FOR PERMISSION TO ENGAGE
IN OUTSIDE EMPLOYMENT

I hereby request that I be granted permission to engage continue to participate in outside employment
as described below:

(Description of Employment)

(Continue on separate page if necessary)

The requested employment will not interfere with my availability for or the proper and effective performance of my duties as an employee of the OIG and will not create or appear to create a conflict of interest with my official duties or reflect adversely on the OIG or the Department of Justice.

I understand that if I maintain outside employment with the same employer in the same or similar capacity as herein requested I must submit a new request for approval annually before January 31 of each year. I also understand that changes in outside employment, including new employment or changes in the duties and responsibilities in previously approved outside employment, must be approved prior to the change taking effect.

If my request for outside employment is approved, I will not use government funds or items purchased or leased with government funds in furtherance of such employment.

I am aware that approval for participation in outside employment may be revoked when continued participation is deemed by the OIG to create or appear to create a conflict of interest, reflect adversely upon the OIG or the Department of Justice, in any manner interfere with my availability for or the proper and effective performance of my official duties, or violate the laws of the United States or the regulations governing Federal and Department of Justice employee activities.

Employee's Name (Please print) _____

Employee's Signature: _____ Date: _____

Concur _____
(Office Head's Name - Please print)

Do Not Concur _____ Date: _____
(Office Head's Signature)

Approved _____

Disapproved _____ Date: _____
(AIG)

Approved _____

Disapproved _____ Date: _____
(General Counsel)

OIG Form I-030/1 (10/18/07)

Revisions

This chapter was originally issued on October 15, 1992, revised on April 7, 2008, and again on April 27, 2012, and now in March 2013.

030.5: The Procedures section has been updated to include the most recent discrimination coverage. This section has also been enhanced to include policy regarding consensual romantic or sexual relationship between a supervisory employee and a subordinate employee.

031.1 Policy. The Office of the General Counsel (OGC) should receive all complaints or allegations of on- or off-duty misconduct or violation of law by any employee of the Office of the Inspector General (OIG).

All OIG personnel, regardless of grade, title, or position, have the responsibility to immediately self-report, in writing, any arrest and any on- or off-duty allegations of misconduct to their supervisor or a higher level official in the chain of command and to the OIG's Security Programs Manager (SPM). This responsibility cannot be waived, delegated, or in any other respect excused.

031.2 Reference.

- A. Inspector General Act of 1978 (Public Law 95-452) as amended;
- B. Inspector General Reform Act of 2008 (Public Law 110-409, October 14, 2008); and
- C. Department of Justice Security Programs Operating Manual (December 21, 2010).

031.3 Scope. The provisions of this directive apply to all employees of the OIG.

031.4 Procedures. This directive sets out the procedures to be followed with regard to all complaints and allegations of on- or off-duty misconduct or violation of law by any employee of the OIG.

- A. OGC should receive all complaints and allegations of misconduct or violation of law by any employee of the OIG.
 - (1) Any OIG employee who learns of or receives any complaint or allegation of misconduct or violation of law by any OIG employee should report such complaint or allegation to the appropriate supervisor. The complaint or allegation should then be reported, through the appropriate chain of command, to OGC. This procedure applies to complaints or allegations discovered by OIG employees or received by the OIG from other DOJ components or the general public. This procedure also applies to the self-reporting of arrests and allegations of misconduct by employees as discussed in the Inspector General Manual (IGM), Volume I, Chapter 030, Standards of Conduct.
 - (2) An OIG employee may, when the employee believes it is appropriate, report the complaint or allegation of misconduct to an Assistant Inspector General (AIG) or to OGC directly. When OGC receives the complaint or allegation directly, it will normally notify the appropriate AIG of the complaint or

allegation, unless such notice is inappropriate given the circumstances of the allegation or complaint. Nothing in this chapter prevents an employee or a supervisor from notifying the Deputy Inspector General (DIG) or the Inspector General (IG) directly of the allegation or complaint, or precludes the IG or DIG from referring the complaint or allegation for investigation by a component of the OIG other than OGC if the complaint or allegation involves an OGC employee, or under other appropriate circumstances.

- (3) Reports to OGC of such complaints or allegations should normally be made in writing or by e-mail, but can be made orally.
 - (4) Normally, within a week of receiving the report of the allegation, OGC will inform the appropriate AIG whether OGC intends to investigate the complaint or allegation, whether the complaint or allegation will be investigated by another OIG division, or whether the complaint or allegation will be referred back to the appropriate OIG division or office for action. OGC may investigate the complaint or allegation with OGC employees or may request assistance from any AIG in conducting the investigation.
 - (5) If OGC refers the allegation back to another OIG division or office for action, OGC shall inform the division or office whether OGC should be kept apprised of the action taken by the division or office in investigating or responding to the complaint or allegation, and the conclusion reached regarding the complaint or allegation.
- B. OGC shall be responsible for notifying the appropriate AIG of the results of any OGC investigation, unless such notice is inappropriate under the circumstances of the complaint or allegation. OGC will also keep the DIG, and when appropriate the IG, apprised of sensitive complaints and allegations and the results of its investigations.
- C. Self-Reporting Allegations of Misconduct and Reporting Violations Relating to Classified and Sensitive But Unclassified (SBU) Information.
- (1) All OIG personnel regardless of grade, title, or position, have responsibility to immediately self report, in writing, any arrest and any on- or off-duty allegations of misconduct to their supervisor or a higher level official in the chain of command and to the OIG's SPM. This responsibility cannot be waived, delegated, or in any other respect, excused.
 - (2) All OIG personnel have the responsibility to safeguard information related to national security to which they have access, and to report to the proper authority the violations by themselves and others that could lead to

unauthorized disclosure of classified and SBU information. The OIG's SPM is a proper authority to whom such violations should be reported.

Revisions

This chapter was originally issued on June 5, 1998. It was revised on July 26, 2007; March 23, 2011; and October 9, 2012.

Title: Revised title to “Complaints, Allegations, and Self-Reporting of Misconduct by OIG Personnel.” Formerly: “Complaints and Allegations of Misconduct by OIG Personnel.”

031.1: Revised Policy section to include information that all OIG personnel are responsible for self-reporting any arrest or misconduct to their immediate supervisor and to the OIG’s Security Programs Manager. OGC will now receive all complaints or allegations of on- or off-duty misconduct or violation of law by OIG employees.

031.2: Added as reference: The Inspector General Reform Act of 2008 (Public Law 110-409, October 14, 2008). Also added reference to the DOJ Security Programs Operating Manual (December 21, 2010).

031.4.A.2: Added the provision that the IG or DIG can refer the complaint of allegation to an OIG component other than OGC under appropriate circumstances.

031.4C: Added information on self-reporting of misconduct and reporting violations relating to classified and sensitive information.

031.5: Responsibilities section was merged into 031.4 Procedures section.

- 102.1 Policy. It is the policy of the Office of the Inspector General (OIG) to comply with applicable law, regulations, and Department of Justice (DOJ) policy and guidelines when responding to Freedom of Information Act (FOIA), Privacy Act (PA), and other requests for documents in the possession of the OIG. This directive sets forth the process for handling requests received by the OIG for information maintained in official OIG files, including requests made pursuant to the FOIA and the PA.
- 102.2 References.
- A. 5 U.S.C. § 552, Freedom of Information Act;
 - B. 5 U.S.C. § 552a, Privacy Act;
 - C. 18 U.S.C. § 1905, Disclosure of Confidential Information Generally;
 - D. 28 C.F.R. Part 16, Subparts A, B, D & E.
- 102.3 Scope. This directive applies to all OIG employees and to any request made for information maintained in OIG files.
- 102.4 Responsibilities. It is the responsibility of the Office of General Counsel (OGC) to record, process, and file all FOIA/PA requests. In addition, as discussed below, the OGC should be consulted before OIG employees respond to non FOIA/PA requests for information from OIG files by other government agencies or in connection with litigation.
- 102.5 FOIA/PA Requests. Upon receipt of any written FOIA/PA request, all divisions or offices shall immediately forward the request to the OGC. All employees should notify anyone making a verbal FOIA/PA request that such requests must be in writing and addressed to the OGC. No OIG employee, absent authorization from OGC (and supervisory approval, as required), shall respond to any FOIA/PA request.
- 102.6 Release of Information to Other DOJ Components. Requests for information by other DOJ components for official purposes are not considered FOIA/PA requests. Employees may share information from OIG files with other DOJ employees who have an official need to know the information without prior consultation with the OGC. Employees should seek supervisory guidance prior to the release of any information.
- 102.7 Release of Information to Other Government Entities. Because the PA or other statutes may limit the information the OIG may release outside the DOJ, employees should consult with OGC before releasing information from OIG files to other government agencies. This provision does not apply to informal requests from the General Accountability Office for general information regarding OIG audits and evaluations.

- 102.8 Release of Information in Connection with Litigation. From time to time OIG employees may be asked to release official information in connection with litigation, e.g., in response to a subpoena or document request. The DOJ has promulgated regulations setting forth the procedures to be followed in response to such requests. In order to ensure compliance with these procedures, any OIG employee who receives such a request should contact the OGC. This provision does not apply to the disclosure of information to federal prosecutors by OIG special agents in criminal prosecutions. In such cases, the special agent should work with the Assistant United State Attorney or other DOJ attorney handling the case.
- 102.9 Record Keeping Requirements When Information is Released Outside DOJ. To comply with certain record keeping requirements imposed by the PA, any time information from an OIG file is released to an individual or entity outside DOJ, a written record of the disclosure should be maintained in the file. This record should include the name and address of the person or entity to whom the information was disclosed as well as the date, nature, and purpose of the disclosure. Accordingly, the OIG division that provides information in response to a particular request will ensure that such information is placed in the file. If a cover memorandum that contains the information listed above is sent to the requestor, placing a copy of that letter in the file will satisfy this record keeping requirement.
- 102.10 Public Release of Audit and Evaluation Reports and Certain Special Reports. It is OIG policy and practice to make most final audit and evaluation reports and certain special reports that address subjects of particular interest and importance available for public review on the OIG's World Wide Web (WWW) site. It is the responsibility of the OGC to review all such reports prior to posting on the WWW site to ensure that they do not contain information that should not be publicly released (e.g., proprietary, confidential, or personal information). Accordingly, before posting any report on the WWW site, the appropriate division shall submit the report to the OGC for review.
- 102.11 Draft Audit and Evaluation Reports. All draft audit and evaluation reports shall contain a legend on the cover page stating that the dissemination of this report is restricted to limited official purposes and that the report may only be shared with DOJ employees for such purposes.
- 102.12 Single Audit Act Reports. When a request (verbal or written) is made for an audit report prepared pursuant to the Single Audit Act, the requester will be referred (similarly verbally or in writing) to the appropriate agency. If such report concerns a state or local entity, the requester will be referred to the Federal Audit Clearinghouse. If the report concerns a non-profit entity, the requester will be referred to that entity.

INSPECTOR GENERAL MANUAL
Volume I, Chapter 102
FOI and PA Request and Procedures
Revisions

FORMAT: this chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives management System.

Deleted § 102.13 as no longer required. Audit does not perform audits of standing and panel trustees.

222.1 Policy. The Office of the Inspector General (OIG) is entrusted with handling sensitive but unclassified (SBU) information. This information must be appropriately safeguarded to comply with applicable laws and regulations and to protect individual rights or critical operations of the OIG or the Department of Justice (DOJ). It is the policy of the OIG to comply with these laws and regulations and provide adequate protection to safeguard SBU information.

Guidance for the processing and handling of classified information and data is addressed separately in Inspector General Manual (IGM), I-220, Document Security.

222.2 Reference. These procedures are in accordance with DOJ Order Nos. 2600.2C, 2600.4, 2610.2A, 2620.5A, 2620.7, 2640.1, and 2640.2E, and the DOJ Security Programs Operating Manual.

222.3 Scope. This chapter applies to all OIG employees and contractors. This chapter provides specific guidance on the processing and handling of SBU information and data and should be read in conjunction with IGM I-220, which provides guidance specific to the processing and handling of classified information and data.

222.4 Responsibilities.

A. The Inspector General (IG) is responsible for:

- (1) specifying through this directive the categories or types of information that originate in the OIG and are designated as SBU;
- (2) identifying those subordinate officials who have authority to determine if information originating under their supervision or cognizance qualifies as SBU or requires protection in excess of the minimum levels established in this directive, and the officials so designated are responsible for ensuring that personnel under their direction are aware how to properly handle, store, and transmit these special designated categories and all categories of information considered SBU.

B. The Security Programs Manager (SPM) has the responsibilities described in DOJ Order 2600.2C and also is responsible for:

- (1) ensuring the safekeeping of SBU material in the OIG;
- (2) overseeing OIG employee and contractor compliance with information security requirements;
- (3) ensuring that OIG contracts adequately incorporate and comply with all information security requirements;

- (4) providing guidance to OIG personnel in information security matters;
 - (5) ensuring that adequate security equipment and storage devices are available; and
 - (6) ensuring that adequate security measures and procedures are implemented to protect SBU information.
- C. Office Heads are the highest level official in each office location. They are responsible for:
- (1) overseeing compliance with information security requirements at the facility;
 - (2) developing office-specific guidance to ensure information originating under their supervision meets the minimum protection levels established in this directive; and
 - (3) designating a primary and alternate Security Officer for the facility.
- D. Security Officers are responsible for protecting SBU information in the facility and maintaining communications with the SPM for local security operations.
- E. Employees and contractors are responsible for the protection and storage of SBU information and materials in their custody.

222.5 Definitions.

- A. Sensitive information is any information of which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of OIG, DOJ, or federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that is not classified as national security information.
- B. The categories or types of sensitive information within the OIG include, but are not limited to, SBU, Limited Official Use (LOU), For Official Use Only (FOUO), and Law Enforcement Sensitive (LES), hereinafter referred to collectively as SBU. In no case should information be designated as SBU or any other sensitivity category to conceal inefficiency, misdeeds, or mismanagement.
- C. The following categories are provided for illustrative purposes only as examples of the types of OIG information considered SBU:

- (1) Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, such as their full name, social security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to a specific individual. Some personal information is not generally considered PII because many people share the same trait, including first or last name, country, state, or city of residence, age, gender, race, name of school and workplace, and grades, salary, or job position;
- (2) specified informant and witness information;
- (3) grand jury information;
- (4) specified investigative material;
- (5) tax information;
- (6) information that could be sold for profit;
- (7) reports that disclose security vulnerabilities;
- (8) information that could result in physical risk to individuals; and
- (9) company proprietary information.

222.6 Procedures.

A. Identification and Markings.

- (1) OIG material that contains information the IG or his designee has determined is SBU must be appropriately identified to ensure that all persons having access to the information outside of the OIG's control are aware of the protection requirement.
- (2) The identification of sensitive information may be accomplished by written instructions or a marking of SBU or another category of sensitive information in one of the following manners:
 - a. on the first page of the material;
 - b. a notation in a covering memorandum;
 - c. use of a cover sheet;

- d. use of a sticker on computer media; or
- e. any other method authorized by the IG.

(3) The purpose of identifying SBU information is to ensure that all recipients of the material not familiar with OIG or DOJ policies are aware that the information requires protection.

B. Storage and Transmission.

(1) General.

- a. Personnel who have custody of material designated as SBU shall exercise care to ensure that the information is not available to individuals who have no legitimate business need for access to the information.
- b. At a minimum, unauthorized individuals must not be able to enter areas unobserved and have visual access to SBU information.

(b) (7)(E)

- d. The sensitivity of some SBU, including but not limited to tax information and grand jury information, may require a higher level of protection. (b) (7)(E)
- Questions regarding information protected under the references listed in Section 222.2 of this directive should be directed to the SPM. Questions regarding categories of information originating within the division described in Section 222.4.A.(2) of this directive should be directed to the appropriate designated official in your division.

(2) Information Technology Systems.

- a. Non-OIG computers, including personally-owned computers, shall not be used to store or process OIG or DOJ data with one exception:

(b) (7)(E)

- b. OIG data are prohibited from being stored or processed on any networked computer outside of the OIG's IGNITE network,

with one exception: (b) (7)(E)



- (3) SBU Taken Out of an OIG Facility.
- a. Electronic files containing SBU, including PII, must be transmitted only on approved encrypted storage devices or on an encrypted OIG laptop computer.
 - b. OIG employees and contractors should transport only the minimum amount of SBU information necessary for their duties. OIG Divisions may develop additional division-specific guidance for removing SBU information from an OIG or DOJ facility. This guidance may require that an inventory of specified types of SBU files being transported be conducted and provided to the supervisor prior to removal from the OIG facility.
 - c. Prior to removing certain SBU information specified by OIG Divisions from an OIG facility, an employee must obtain the supervisor's approval.

(b) (7)(E)



(4) Custody of SBU While on Official Travel

(b) (7)(E)



- b. SBU must not be reviewed in public places where people without a “need to know” can inadvertently view either documents or information on an OIG laptop computer.

(b) (7)(E)



(b) (7)(E)



C. Access and Dissemination.

(1) Access.

- a. No OIG personnel or non-OIG personnel, including but not limited to contractors, may be given access to SBU information unless that

person has the appropriate background investigation and a need-to-know for the performance of official duties.

- b. Access to SBU information should be maintained at the minimum number of persons consistent with operational requirements.
- c. OIG employees, including students and contractors, will be considered eligible for access to SBU information after a favorable personnel security determination has been made by the Director, Justice Management Division, Security and Emergency Planning Staff in accordance with Executive Order 10450 and IGM I-201, Personnel Security.

(2) Dissemination.

- a. When disseminating hard copy documents that contain SBU, including but not limited to PII, OIG employees must protect the information from unauthorized use, disclosure, and visual access.

(b) (7)(E)



b.

- c. SBU must not be left openly visible in common work areas that regularly receive visitors, such as reception areas, conference rooms, and mailrooms.

D. Destruction and Reuse.

(1) Document Destruction.

- a. SBU documents must be destroyed by shredding or other methods such as burning or pulping.

There is no minimum size requirement for the residue of shredded SBU documents, as there is with National Security Information, so

all single-cut or cross-cut shredders are sufficient for destruction of these documents.

(b) (7)(E)



(2) IT Systems and Media Destruction.

- a. IT systems that have processed, stored, or transmitted SBU or classified information shall not be released from the OIG's control until the equipment is sanitized by degaussing and removal of all memory components. This requirement includes equipment donated to schools and other organizations.

OIG contractors are responsible for providing the COTR with a written certification that all DOJ data has been removed prior to releasing equipment from the contractor's control.

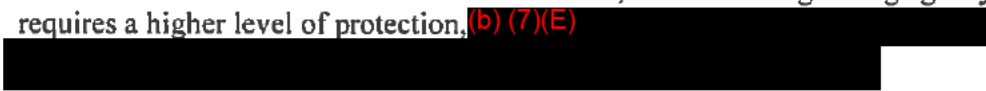
- b. OIG IT equipment under maintenance warranty contracts shall include stipulations that equipment removed from OIG offices shall be sanitized before removal.
- c. When no longer usable, diskettes, tape cartridges, ribbons, and other similar items used to process SBU and classified information shall be destroyed by being overwritten with nonsensitive data, degaussed, shredded, or incinerated, whichever method is available, appropriate, and cost effective.
- d. When no longer usable, compact disks used to process SBU shall be destroyed by shredding, using a CD destroyer, or physically breaking the disk into pieces.

(3) IT Removable Media Reuse.

When no longer required for mission or project completion, IT storage media that will be re-utilized by another person within the OIG shall be overwritten with software and protected consistent with the data sensitivity level at which they were previously used.

E. SBU Collected and Provided by Other Agencies.

Sensitive materials and data provided by other agencies must be maintained in accordance with Section 222.6B of this directive, unless the originating agency requires a higher level of protection. (b) (7)(E)



F. Incident Reporting and Handling Requirements.

(1) Reporting the Loss or Theft of SBU.

- a. OIG employees and contractors must report the loss or theft of sensitive materials and data, whether in document or electronic format, to their supervisor or COTR, or designated higher level official, as soon as the loss or theft is determined.
- b. The supervisor or COTR and office head must collect the facts surrounding the loss and the extent of any potential damage from the loss and report the incident immediately to the SPM and Information Systems Security Officer (ISSO) and provide periodic updates as additional information is developed.
- c. The SPM and ISSO must report the loss of SBU and the extent of any potential damage from the loss to the DOJ Computer Emergency Readiness Team (DOJCERT) within one hour after they receive notification of the loss or theft and provide periodic updates as additional information is developed. DOJCERT will report DOJ incident information, common vulnerabilities, and threats to OMB and US-CERT when required.

(2) Handling Requirements.

In addition to reporting to DOJCERT, the SPM and affected Division must assess the potential damage that may be caused by the loss of SBU and make a determination if it is also necessary to notify originating agencies or affected individuals of the possible security breach.

A security breach includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where persons other than authorized users and for an other than authorized purpose have access or potential access to SBU, including PII, whether documents or electronic data.

- (3) Compliance.
 - a. Compliance with this policy will be enforced through sanctions commensurate with the level of infraction if it is determined that employee negligence was a factor in the loss or breach.
 - b. An appropriate disciplinary action may be imposed depending on the severity of the violation.

- 225.1 **Policy.** Civil remedies include actions to recover damages incurred by the government and to protect agencies from individuals and entities who are deemed to be unfit to do business with the government. In order to implement the various civil remedies available to the government, the civil aspects of audits, inspections, and investigations conducted by the OIG will be pursued vigorously.
- 225.2 **References.** This chapter is issued pursuant to the authority contained in the Inspector General Act of 1978, 5 U.S.C. app, as amended by the Inspector General Act Amendments of 1988 (Pub. L. No.100-504), 102 Stat. 2515, **Attorney General Order 2492-2001, and 28 CFR Part 0.29.**
- 225.3 **Scope.** The provisions of this chapter shall apply to all employees in the Office of the Inspector General (OIG).
- 225.4 **Responsibilities.** **The Fraud Detection Office (FDO) of the Investigations Division is responsible for investigating allegations of fraud and overcharging in connection with contracts and grants awarded by a component of the Department of Justice (DOJ). The Office of the General Counsel (OGC) provides guidance on the civil aspects of matters uncovered during the course of an audit, inspection, or investigation.**
- 225.5 **Procedures.** **Any matter arising out of a DOJ contract or grant that involves a potential monetary loss to the government or might lead to a suspension or debarment of the contractor or grantee shall be referred to the FDO.**
- 225.6 **Civil Remedies.** The following are the most common civil remedies available to the government.
- A. **False Claims Act (31 U.S.C. 3729) (FCA).** The FCA provides for the recovery of triple damages and up to a \$10,000 civil penalty for each false claim for payment knowingly submitted to the government and/or for each false statement knowingly submitted in support of a false claim.
- (1) **Persons Subject to the FCA.** A "person" under the FCA includes an individual, corporation, partnership, nonfederal government entity, or grantee.
 - (2) **Claim.** A claim includes any claim or statement in support of a claim for the payment of money, the transfer of property, or the grant of a benefit, including a claim to have the government forgo the collection of a debt or duty to pay.
 - (3) **Making or Causing a Claim to be Made Upon or Against the Government.** A "person" may be liable for making a false claim or for causing another to make a false claim. For example, a subcontractor is liable under the FCA for submitting a false claim to a prime contractor who, without knowledge of its falsity, submits the claim for payment to the government.

- (4) **Intent.** No proof of specific intent to defraud is required to establish liability under the FCA. It must be established that the party acted with knowledge that the statement or claim was false or in reckless disregard for its truth.
 - (5) **Double Jeopardy.** Actions brought under the FCA are "remedial"; hence, no double jeopardy claim can be made when an FCA suit is brought after conviction or acquittal under federal criminal false claims or statements statutes (e.g., 18 U.S.C. 286, 287, 371, or 1001).
 - (6) **Statute of Limitations.** An FCA suit must be initiated within the latter of six years from submission of the claim or three years after the government knew or reasonably should have known of the falsity of the claim but not more than 10 years from the date of the violation.
 - (7) **Qui Tam.** Individuals may bring a false claim action ("qui tam" suit) on behalf of themselves and the government and share in any recovery obtained. The suit is filed under seal and the government has sixty days from the date of the filing to decide whether to intervene and take over the action. If the suit involves DOJ, the OIG will be asked to conduct an investigation to assist government counsel to decide whether or not to take over the case.
- B. Program Fraud Civil Remedies Act (31 U.S.C. 3729) (PFCRA).** The PFCRA provides a forum, presided over by an administrative law judge (ALJ), to hear false claim and false statement cases involving damages for claims or groups of related claims of \$150,000 or less.
- (1) **Elements.** Except as noted below relative to damages and the statute of limitations, the elements of a claim under the PFCRA (i.e., what is a claim, who is subject to liability, intent, etc.) track the FCA.
 - (2) **Damages.** Liability under the PFCRA is double the government's damages plus civil penalties of \$5,000 for each false claim or statement.
 - (3) **Statute of Limitations.** For liability under the PFCRA, a notice of hearing must be served on the defendant by the presiding official within six years of the date of submission of the false claim or statement.
 - (4) **Investigating Official.** The OIG of DOJ is responsible for investigating claims under PFCRA and referring its findings to DOJ's reviewing official (RO).
 - (5) **Reviewing Official.** The General Counsel, Justice Management Division (JMD), is the DOJ's RO. The RO is responsible for reviewing the Report of Investigation and transmitting a written request for authority to initiate a

proceeding under the PFCRA to the Fraud Section of the Commercial Litigation Branch of the Civil Division.

- (6) **Adjudicating Official.** An ALJ will conduct a hearing to determine whether a defendant is liable under the PFCRA.
- C. **Civil RICO.** 18 U.S.C. §§ 1964-1968 (Racketeer Influenced and Corrupt Organizations) provides for civil remedies against a person who has received any income from a pattern or practice of racketeering activity or through the collection of an unlawful debt. The United States may recover damages and seek equitable relief, including ordering a person to divest any interest in an enterprise or restricting future activities and investments. Civil action requires the prior approval of the Criminal Division of DOJ.
- D. **Anti-Kickback Act.** 41 U.S.C. §§ 51-58 prohibits payment of any kind to or by a contractor for the purpose of receiving any favorable treatment in connection with a government contract. A knowing participant in a kickback is liable for double damages and up to \$10,000 in civil penalties for each violation.
- E. **Contract Disputes Act.** 41 U.S.C. § 604 provides for the recovery of the amount of a claim or portion thereof, which is presented to a contracting officer for payment and which is based upon fraud or misrepresentation. **The** contractor is liable for the amount of the false and unsupported portion of the claim whether or not it has been paid by the government. A claim must be in writing, and certified and **the** contractor must know that **the** claim is false. **The** government may also recover **the** cost of investigation.
- F. **Bribery and Conflict of Interest.** The government may seek recovery of any amount paid or received for bribery or conflict of interest from both the payer and payee of the bribe under common law principles. Pursuant to 18 U.S.C. § 216, the Attorney General may seek to recover from the recipient of a bribe the amount of the bribe, a \$50,000 civil penalty for each violation of the criminal bribery statutes, and to obtain injunctive relief.
- G. **Debt Collection Act.** The Debt Collection Act of 1982 (5 U.S.C. 5514; 31 U.S.C. 3701, 3711, 3716-19; 4 C.F.R. 102) gives agencies broad powers to collect claims through (a) the offset of a federal employee's salary for indebtedness to the United States and (b) administrative offset of money payable by the government, to satisfy a debt the person owes the government. Prior to collection, the purported debtor has an opportunity to challenge the agency's determination that a debt exists.
- H. **Victim and Witness Protection Act.** The Victim and Witness Protection Act of 1982 (Title 18 U.S.C.1501) ensures restitution for victims of federal crimes, including the government. A court's decision on whether to order restitution and in what amount

relies upon pre-sentence investigation reports prepared by the U.S. Probation Officers.

- I. Suspension and Debarment. Suspension and debarment are measures taken to disqualify contractors from participating in government contracting. The Federal Acquisition Regulations (FAR) 48 CFR § 9.4 authorize the imposition of a government wide suspension or debarment upon a finding that a contractor has committed an offense indicating a lack of business integrity or business honesty that seriously and directly affects its present responsibility.

A suspension is a temporary measure of no longer than 18 months. A debarment is for a fixed period of up to three years. Suspension and debarment are prospective only. They affect a contractor's ability to enter into new contracts. They do not affect ongoing work under an existing contract.

The role of the OIG is to investigate allegations of contractor misconduct, report its findings to the contracting component, and in concert with the contracting component make a recommendation regarding suspension or debarment to JMD.

001.1 Policy. This chapter describes the organization, mission, and authorities of the Investigations Division (INV) of the Department of Justice (DOJ) Office of the Inspector General (OIG).

The Assistant Inspector General for Investigations and the executive staff of the INV will clearly communicate the mission, organization, and law enforcement authorities of the OIG and the INV to their employees, DOJ, the executive branch, and the Congress.

All employees of the INV will perform their duties in accordance with the authority granted to them, as enumerated above, and ensure that their conduct does not exceed such authority.

001.2 Reference. This policy is issued under the provisions of the following:

- A. The Inspector General Act of 1978 (Public Law 95-452, October 12, 1978), as amended by the Inspector General Act Amendments of 1988 (Public Law (Pub. L.) 100-504, October 18, 1988), and Attorney General Order No. 1341-89, dated April 14, 1989 (establishes the OIG).
- B. The USA Patriot Act of 2001 (Pub. L. 107-56) (establishes OIG responsibility to receive and investigate allegations of civil rights and civil liberties abuses arising under the Patriot Act).
- C. The Homeland Security Act of 2002 (Pub. L. 107-296) (establishes statutory law enforcement authority for OIG special agents) and Attorney General Guidelines for Inspectors General with Statutory Law Enforcement Authority, dated December 8, 2003.
- D. The 21st Century Department of Justice Appropriations Authorization Act (Pub. L. 107-273, November 2, 2002); parts 27.3 and 0.29, title 28, of the Code of Federal Regulations; and Attorney General Order 2492-2001 (establishes OIG authority to investigate misconduct within all components and delineates the OIG relationship with the Office of Professional Responsibility).

001.3 Scope. The provisions of this chapter apply to all employees of the INV.

001.4 Procedures. The INV Headquarters will maintain and disseminate an up-to-date division organizational chart (See the posting on the intranet).

001.5 Mission Statement. The INV will provide leadership and assist in promoting economy, efficiency, and effectiveness within the DOJ; enforce the fraud, waste, abuse, and integrity laws and regulations of the United States within DOJ; and bring to the criminal and civil justice system of the United States or to any other competent jurisdiction those individuals or organizations involved in financial, professional, or criminal misconduct relating to DOJ programs and operations.

001.6 Mission Responsibilities. The primary responsibilities of the INV include:

- A. Investigating alleged violations of the fraud, abuse, and integrity laws that govern DOJ or that cover operations that are financed by DOJ. Preparing for criminal prosecution those violations that can be proven and investigating allegations for possible civil or administrative action.
- B. Reporting to the Inspector General (IG) on problems and deficiencies in the administration of DOJ programs or operations, or DOJ-financed programs or operations. Recommending corrective action and monitoring the progress made in implementing such action.
- C. Coordinating and cooperating with federal, state, and local government agencies, as well as non-government entities, in order to:
 - (1) Promote the economic and efficient administration of DOJ programs and operations.
 - (2) Prevent and detect fraud, waste, and abuse in DOJ programs and operations.

001.7 Law Enforcement Authorities. Special agents of the OIG are empowered with broad law enforcement authorities under the Inspector General Act of 1978 (title 5 appendix of the United States Code), as amended. These authorities may be exercised when reasonably related to the performance of the duties, functions, and responsibilities assigned to the IG. Therefore, in order to prevent and detect fraud, abuse, and misconduct within DOJ and its programs and operations, an OIG special agent is authorized to:

- A. Carry firearms (see the Inspector General Manual (IGM), Volume III, "Investigations," Chapter 201 (IGM III-201)).
- B. Seek and execute arrest warrants (see IGM III-232).
- C. Seek and execute search warrants (see IGM III-233).
- D. Arrest without a warrant any person for any felony offense committed in the agent's presence or arrest without a warrant any person for any felony offense committed outside of the agent's presence if the agent has reasonable grounds to believe that the person to be arrested has committed or is committing such a felony (see IGM III-232).
- E. Transport arrestees in the custody of the Attorney General.
- F. Serve subpoenas issued under authority of the Inspector General Act or issued by a federal grand jury or federal court (see IGM III-230).

- G. Serve legal writs, summons, and complaints.
- H. Have access to all records, reports, audits, reviews, documents, papers, recommendations, and other materials that relate to the programs and operations of DOJ.
- I. Administer or take from any person an oath, affirmation, or affidavit.

001.8 Inquiries Concerning Law Enforcement Authorities. Official inquiries concerning the scope of law enforcement authorities should be directed to the Deputy Assistant Inspector General for Investigations, who will coordinate any response with the General Counsel.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 001
Organization and Mission
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was originally issued on 5/19/97 and was re-written to reflect updates and/or changes in policies, laws, and/or guidelines.

032.1 **Policy.** This chapter addresses Department of Justice (DOJ) Office of the Inspector General (OIG) policy on the issuance of news releases and other communications with the media or the public regarding OIG activities. This chapter should be read in conjunction with Inspector General Manual (IGM) volume I, chapters 032, “Public Affairs,” and 102, “Freedom of Information and Privacy Act Requests and Procedures.”

All communications with the media should be reported to and, in certain instances, previously coordinated with the Assistant Inspector General for Investigations (AIGI). In addition, certain matters may also require coordination with the OIG Immediate Office (Immediate Office), DOJ’s Office of Public Affairs (OPA), or the affected federal prosecutor. All communications with OPA will be initiated by the OIG Immediate Office. Communications with a United States Attorney’s Office (USAO) or the DOJ Criminal Division or Civil Division may be initiated by the field special agent in charge (SAC) or Investigations Division (INV) Headquarters.

- A. Field SACs may release information to the local media as long as applicable DOJ and OIG guidelines are followed. Communications with the media in appropriate situations are a positive means of advising the public of the mission and work of the OIG.
- B. It should be recognized that communicating with the press regarding OIG investigative matters requires balancing of the interest of a defendant, including the right to a fair trial, with the public’s right to know about the conduct of law enforcement activities, the interests and safety of victims and witnesses, and the government’s ability to administer justice. These interests must be considered before issuing any public comment regarding a particular matter.

032.2 **Reference.** This chapter is issued in accordance with DOJ policy contained in 28 C.F.R. § 50.2.

Authority to speak to the media, as set forth in this chapter, is delegated to the Deputy Inspector General (DIG) and other designated staff of the Immediate Office, the AIGI, the Deputy Assistant Inspector General for Investigations (DAIGI), and SACs. No other INV personnel are authorized to speak to the media on behalf of the OIG without the prior approval of the AIGI. This restriction does not apply to an employee disclosing to the media information for which protection is provided under 5 USC § 2302(b)(8)(A). See IGM Vol. I, section 032.5E.

032.3 **Scope.** The provisions of this chapter apply to all employees of the INV.

032.4 **Procedures.** The sections of this chapter prescribe procedures for specific aspects of media relations.

032.5 **Media Requests That Must Be Referred to or Coordinated With Investigations Division Headquarters.** The following types of media requests require coordination with INV

Headquarters, which in turn will coordinate with the DIG or the Immediate Office's designee before any information is released:

- A. News of International/National/Major Regional Interest. Any issues of national, international, or major regional interest require coordination with INV Headquarters, which will in turn notify the Immediate Office. The Immediate Office should be informed as far in advance as possible about any issue that might attract international, national, or major regional media interest before anyone speaks with the media.
- B. Requests from National or Significant Media Organizations. INV Headquarters must be immediately informed of all inquiries from national media organizations or newspapers from large cities, regarding in-depth stories or other matters affecting the OIG or DOJ. Examples include television (for example, Good Morning America, 60 Minutes), radio (for example, National Public Radio syndicated programs), newspapers (for example, New York Times, Wall Street Journal, Washington Post, Los Angeles Times), magazines (for example, Newsweek, Time), and national wire services (for example, UPI, AP, Gannett, Reuters). The SAC will report to INV Headquarters and the Immediate Office if he or she believes any matter will receive more than local media attention.

Accordingly, if a media representative contacts a field office seeking information regarding a national or significant regional issue, the SAC should refer the media representative to the Immediate Office and promptly inform both INV Headquarters and the Immediate Office about the nature of the inquiry. If the inquiry concerns an ongoing investigation or pending prosecution, the SAC shall also notify the responsible prosecutor and the USAO public affairs representative.

- C. News Conferences. Attendance at any news conference by a member of the OIG must be coordinated in advance with INV Headquarters, which will in turn coordinate with the Immediate Office.
- D. Comments on Specific Issues (Legislative Proposals, Budget). Media inquiries regarding existing, new, or pending matters, such as legislative or budget proposals or policies, must be forwarded to INV Headquarters, which will then coordinate an appropriate response through the Immediate Office.

032.6 Media Contacts and Release of Information by Field Office SAC. DOJ regulations, including 28 C.F.R. § 50.2, permit certain information regarding ongoing criminal or civil cases to be reported publicly.

- A. Inquiries Regarding Federal Prosecutions and Litigation. Each United States Attorney is responsible for all press relations concerning prosecutions or litigation involving his or her office. Accordingly, any OIG communication with the media, such as a press release or oral statement, concerning an arrest for a crime that will

be prosecuted by a USAO or other DOJ element (for example, the Public Integrity Section or the Civil Rights Division) must first be coordinated with the appropriate USAO or DOJ representative.

- B. Release of Information Regarding Ongoing Investigations. No public comments regarding investigative activities may be made before an arrest and charge (by information, indictment, or complaint, either civil or criminal) against an individual or entity unless an incident has received substantial publicity, the community needs to be reassured that law enforcement efforts have been initiated, or a statement is in the interest of public safety. In those instances, any statement to the media shall be coordinated with INV Headquarters and the Immediate Office before its issuance.
- C. Disclosure After Arrest and a Criminal Complaint, Indictment, or Information Has Been Issued. Consistent with the policies and requirements set forth in this chapter, including advance coordination with INV Headquarters and the USAO, designated OIG employees may disclose the following information after an arrest and criminal complaint, indictment, or information has been issued:
- (1) defendant's name, age, residence, employment, marital status, nationality, and similar background information;
 - (2) the substance or text of the charge, such as a complaint, indictment, or information;
 - (3) the identity of the investigating or arresting agency or office and the length or scope of the investigation;
 - (4) the circumstances immediately surrounding the arrest, including the time and place, resistance, pursuit, possession and use of weapons, and description of physical items seized at the arrest. However, if any background data relating to the circumstances of the arrest would be unduly prejudicial or serve no law enforcement function, such information shall be withheld; and
 - (5) a statement explaining that the charge is merely an accusation and that the defendant is presumed innocent unless and until proven guilty.

See Appendix A for a sample press release.

- D. Release of Criminal History Information. No OIG employee may disseminate to the media any information concerning a subject's prior criminal record except as set forth in this paragraph. Where a prior conviction is an element of the current charge, such as in the case of a felon in possession of a firearm, designated OIG employees may confirm the identity of the subject and the general nature of the prior charge when such information is part of the public record in the case at issue.

In certain extraordinary situations, such as a search for a fugitive or in extradition cases, OIG employees may confirm the identity of a subject and the prior offenses.

- E. Information That Should Not Be Released Regarding Criminal Investigations. Disclosures should contain factual data and should not include any subjective observations or opinions. No information may be released to the media for the purpose of influencing the outcome of a trial. The following types of information would not serve a significant law enforcement function and would tend to raise the specter of prejudice and, therefore, should not be included in any public statement or discussion:
- (1) observations or opinions regarding a defendant's character;
 - (2) statements, admissions, confessions, or alibis that are attributable to a defendant; the refusal or failure of the defendant to speak of these matters;
 - (3) references to investigative techniques, such as polygraph evidence, fingerprints, ballistic tests, laboratory analyses, or to the refusal of the defendant to submit to such tests;
 - (4) statements concerning the identity, testimony, or credibility of any witness;
 - (5) statements concerning evidence or argument, regardless of whether such data or argument will be presented at trial; and
 - (6) opinions as to the defendant's guilt or the possibility of a guilty plea to a charged offense or to a lesser offense.
- F. Release of Information Regarding Civil Litigation. During an investigation or litigation involving civil matters, a designated OIG employee may issue, with appropriate coordination with the USAO or DOJ representative, a civil litigation statement that is based on a quotation from or reference to public records.
- G. Information That Should Not Be Released Regarding Civil Matters. INV employees may not issue a statement when there is a reasonable likelihood that such dissemination will interfere with a fair trial or the information relates to:
- (1) the evidence regarding the occurrence or transaction in issue;
 - (2) the character, credibility, or criminal records of a party, witness or prospective witness;
 - (3) the performance or results of any examinations or tests or the refusal or failure of a party to submit to such examinations or tests;
 - (4) an opinion as to the merits of the claims or defenses of a party; and

- (5) any other matter reasonably likely to interfere with a fair trial in the matter at hand.

032.7 Assisting/Deterring News Gathering. Unless directed by court order, OIG employees must not prevent the lawful efforts of the news media to photograph, tape, record, or televise an arrestee or a sealed crime scene from outside the sealed perimeter. However, if news media are present at the scene of an execution of a search or arrest warrant, OIG personnel may request that the media withdraw if the media presence puts the operation or the safety of individuals in jeopardy.

- A. OIG employees shall take no action to encourage or assist news media in photographing a defendant or accused person. Employees may not provide photos of defendants to the media unless a legitimate law enforcement purpose will be served (such as the photograph of a fugitive).
- B. If any critical incident occurs, such as a shooting involving an OIG employee, no OIG employee should identify or confirm the identity of an OIG employee involved in such an incident to the media.

032.8 Record of Media Coverage. To the extent available, copies of all local media articles or interview tapes pertaining to INV should be forwarded to INV Headquarters, which will provide a copy to the Immediate Office.

032.9 Publications or Speeches by Investigations Division Personnel. Articles and speeches by INV personnel provide an opportunity to heighten the awareness of the public and other governmental agencies to the OIG's mission and accomplishments. However, such articles or speeches can also create an opportunity for criticism and adverse reactions. Therefore, it is essential that the following policies and procedures are followed before any article or speech is submitted for publication or presentation:

- A. Excluding routine integrity awareness briefings and speeches regarding the OIG and its mission, structure, or jurisdiction, all proposed articles and speeches shall be submitted to the AIGI or DAIGI for review and comment. In addition, the special agent in charge to whom the speaking employee reports must be notified of the employee's intentions and given the opportunity to review the materials before the materials are forwarded to INV Headquarters.
- B. The AIGI or DAIGI should forward the prospective article to the OIG General Counsel or the Immediate Office for review and comment.
- C. Generally, an employee may use his or her official title in connection with an article or speech only if the employee is acting in his or her official capacity as a representative of the DOJ or the OIG. If the material is related to a private communication (for example, a letter to the editor), the employee may not use his or her official title.

- D. In private communications, articles, and speeches, a disclaimer shall be included that indicates that the materials presented are those of the employee and not necessarily those of the DOJ or OIG. This also may be necessary in officially released materials, depending on the circumstances.

- E. Although articles or speeches totally unrelated to an employee's work with the OIG do not require prior review, each INV employee must understand that it is virtually impossible to separate personal and professional identities. Therefore, notification should be made through the employee's chain of command whenever an employee is intending to make a speech or submit an article for publication.

APPENDIX A

Sample Press Release



Department of Justice

FOR IMMEDIATE RELEASE
MONDAY, APR. 25, 2005
WWW.USDOJ.GOV

CRM
(202) 514-2008
TDD (202) 514-1888

PHOENIX DEA AGENT SENTENCED FOR MAKING FALSE STATEMENTS

WASHINGTON, D.C. – Assistant Attorney General Christopher Wray of the Criminal Division and Inspector General Glenn A. Fine announced today that Douglas C. Furlow, 43, a special agent with the Phoenix Field Division of the DEA, was sentenced today by United States District Judge Mary H. Murguia to _____. Furlow pleaded guilty on January 14, 2005, to making a false statement, a violation of 18 U.S.C. § 1001, when he denied to a DEA investigator that he did not try to obstruct an undercover DEA drug investigation by calling and tipping off a drug dealer that he was under surveillance, was meeting an undercover informant, and would be arrested. Prior to his guilty plea, Furlow had been indicted by a District of Arizona grand jury for witness tampering, a violation of 18 U.S.C. § 1512(b)(3).

The charges against Furlow relate to phone calls Furlow made on August 26, 2002. That day, an undercover DEA informant was scheduled to meet the drug dealer to make a drug buy leading to arrest. To block the investigation, Furlow made a series of unauthorized calls to the trafficker and warned of the informant's affiliation with law enforcement. Consequently, the DEA investigation was aborted, and neither the drug buy nor the arrest could be made that day.

This prosecution was handled by Trial Attorneys Kartik K. Raman and Shaun H. Palmer of the Public Integrity Section of the Department of Justice, Washington, D.C., headed by Noel L. Hillman, chief. The investigation was conducted by the Denver Field Office of the Office of the Inspector General, Department of Justice, and the DEA Office of Professional Responsibility, Western Field Office.

###

For additional information, contact: _____ at tel: _____

05-XXX

INSPECTOR GENERAL MANUAL
Volume III, Chapter 032
Media Relations
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was originally issued on 5/19/97 and was re-written to reflect updates and/or changes in policies, laws, and/or guidelines. It had a partial revision on May 23, 2017.

Section 032.2: Added “on behalf of the OIG” as well as the last two sentences in the section.

- 100.1 **Policy.** This chapter establishes administrative policies and procedures to facilitate the orderly operation of the Investigations Division (INV), Office of the Inspector General (OIG).
- 100.2 **Reference.** The Inspector General Act of 1978, as amended; Department of Justice (DOJ) Records Disposition Authority relating to the OIG, dated August 10, 1999; Authority of the Inspector General to establish standardized internal administrative procedures within the OIG.
- 100.3 **Scope.** The provisions of this chapter apply to all employees in the OIG INV.
- 100.4 **Administrative Recordkeeping.**
- A. **File Numbering.** All OIG administrative files will be maintained according to the numbering system that corresponds with the organization of the Inspector General Manual (IGM). Administrative files will contain all related policy and procedure documents and all related incoming and outgoing correspondence. For example, all official travel matters would be filed under IGM, Volume V, Chapter 040 (V-040), and all polygraph matters would be filed under IGM III-265.
- B. **Document and Correspondence Numbering.** The originator of any correspondence or administrative document is responsible for designating the appropriate file number and ensuring that number appears on the document in the upper right portion of the first page.
- 100.5 **Investigative File Retention, Storage, and Disposition.** Investigative files must be maintained in a logical, current, and efficient manner and must be safeguarded from destruction or from disclosure to those who are without appropriate clearance or need to know. Investigative files consist of all complaints and information developed during investigations of known or alleged fraud, abuse, irregularities, or violations of law or regulations. Investigative files may comprise correspondence, notes, attachments, exhibits, working papers, memoranda of investigation, investigative reports, and related documents maintained on paper records or electronic media or both.
- A. **Complaints Classified as Management Referrals or Informations.** Complaints classified as management referrals ("M") or informations ("F") in the Investigations Data Management System II (IDMS II) will be maintained in the field office in numerical order according to the complaint number assigned by IDMS II.
- (1) These complaints will be considered inactive as of September 30 of the fiscal year in which they received their classification. Field offices will retain these files for 5 fiscal years after the inactive date.
- (2) Once this retention period has expired, the related files (with predicated material) should be destroyed by the local field office.

- a. Example 1 – A complaint classified as “M” or “F” in April 2004 becomes inactive on September 30, 2004. The file should be destroyed on or after September 30, 2009.
 - b. Example 2 – A complaint classified as “M” or “F” in November 2004 becomes inactive on September 30, 2005. The file should be destroyed on or after September 30, 2010.
- (3) The file destruction and date of destruction must be documented in the related IDMS II complaint record in the “Remarks” section.
- B. Complaints Classified as Monitored Referrals.** Complaints classified as Monitored Referrals (“R”) in IDMS II will be maintained in the appropriate INV Headquarters office (for example, the Operations Branch or Special Operations Branch, depending on the DOJ component involved) or field office in numerical order according to the complaint number assigned by IDMS II.
- (1) These complaints and any relating files will be considered inactive as of September 30 of the fiscal year in which they are closed (that is, upon receipt of an acceptable response from the component). Offices will retain these files for 5 fiscal years after the inactive date.
 - (2) After this retention period has expired, the files (with predicated material) should be destroyed by the INV Headquarters branch or field office having jurisdiction over the records.
 - a. Example 1 – A complaint classified as “R” in April 2004 and closed in August 2004 (upon receipt of component response) becomes inactive on September 30, 2004. The file should be destroyed on or after September 30, 2009.
 - b. Example 2 – A complaint classified as “R” in April 2004 and closed in November 2004 (upon receipt of component response) becomes inactive on September 30, 2005. The file should be destroyed on or after September 30, 2010.
 - (3) The file destruction and date of destruction must be documented in the related IDMS II record in the “Remarks” section.
- C. Record Destruction Methods.** Destruction of files, as described in paragraphs A and B above, must comply with DOJ security regulations. (b) (7)(E)
- [REDACTED]
- [REDACTED] Field offices should use the office procurement card to pay for file destruction. If the vendor will not accept the office

procurement card, the field office should contact INV Headquarters (Administrative Support Branch) for assistance.

- D. Complaints Classified as Investigations. Open and closed case files will be maintained separately in a secure file room in numerical order according to the complaint/case number assigned by IDMS II.
- (1) **Case File Retention – Complaints classified as Investigations (“I”) will be considered inactive as of September 30 of the fiscal year in which they are closed. Field offices will retain investigative case files for 5 years after the inactive date.**
 - (2) **After Retention Period – At the end of the retention period, the files (with all related material and notes) will be sent to a designated record storage facility. Refer to Appendix A for the name and address of the storage facility currently used by the OIG. This facility will store the files for 10 fiscal years after the inactive date, at which time they will be destroyed.**
 - a. **Example 1 – A complaint classified as “I” in April 2004 and closed in August 2004 (upon completion of all investigative activity) becomes inactive on September 30, 2004. The file should be sent to the record storage facility on or after September 30, 2009 with a designated destruction date of September 30, 2014.**
 - b. **Example 2 – A complaint classified as “I” in April 2004 and closed in November 2004 (upon completion of all investigative activity) becomes inactive on September 30, 2005. The file should be sent to the record storage facility on or after September 30, 2010 with a designated destruction date of September 30, 2015.**
 - (3) **Remarks Entry – The date transferred, the complete box number and the designated destruction date must be entered in the IDMS II “Remarks” section under the case number.**
 - (4) **Packing and Sealing Boxes – Only files classified as an Investigations (“I”) will be sent to the record storage facility. Files should be packed in approved boxes or boxes supplied by the storage facility. Each box must contain only files with the same destruction date. Boxes will be sealed using heavy-duty packing tape.**
 - (5) **Marking and Numbering the Boxes – Each field office will number its boxes consecutively by fiscal year. Sample box marking/numbering and a list of field/area office designators to be used in box numbering are contained in Appendix A.**
 - a. **Boxes must be marked on both ends with the following:**

Box number: consists of the fiscal year, the field office designator, and the consecutive box number. This number contains a maximum of seven digits.

Box numbers are extremely important because if a box is sent with a duplicate number, the storage facility's record for the original box will be erased, and the facility may never be able to locate the original box. Thus, boxes should be numbered consecutively throughout the fiscal year, only starting over with box 01 for the first box sent in a new fiscal year.

- b. Destruction date: 10 years from the inactive date as described above.
 - c. Customer number: See Appendix A.
- (6) Documenting the Box Contents – Each time a box or group of boxes is sent to the record storage facility, the field office must prepare an original and two copies of OIG Form III-100/6 (Inventory Transmittal) (Appendix B). The OIG Form III-100/6 must include:
- a. each box number contained in the shipment;
 - b. OIG case file numbers for all files contained in each box;
 - c. file closing dates;
 - d. designated destruction date for each box.

The original OIG Form III-100/6 will be sent with each shipment of boxes. One copy will be maintained in the field office and one copy will be sent to INV Headquarters.

(b) (7)(E)



- E. Exception to Disposition of Complaints Classified as Investigations ("I"). All records discussed above are classified as "temporary" by the National Archives and Records Administration and thus eventually may be disposed of. However, some investigative case files are of significant value and are said to be "permanent" records. Case files of significant value are those where the case: attracts national

media attention, results in a congressional investigation, or results in substantive changes in DOJ policies and procedures.

- (1) The Assistant Inspector General for Investigations (AIGI) will designate which files will be included in this category upon the advice of the field office special agent in charge (SAC).
- (2) Files meeting the above criteria will be considered inactive as of September 30 of the fiscal year in which they are closed. Files will be retained in the field office for 5 fiscal years after the inactive date.
- (3) At the end of the field office retention period, the entire investigative file will be sent to INV Headquarters. INV will, in turn, transfer the file to the Washington National Records Center (WNRC) in Suitland, Maryland. WNRC will retain the file for 10 years, after which the file will be transferred to the National Archives for permanent retention.

- F. Investigations of Sexual Abuse in Confinement Settings. Written reports of criminal or administrative investigations of sexual abuse and harassment in confinement settings will be retained for as long as the alleged abuser is incarcerated or employed by the agency, plus 5 years. All relevant reports and exhibits will be uploaded to iManage for document retention purposes. (See also Appendix F for definitions of sexual abuse and harassment terms.)

100.6 Time and Attendance. OIG policies and procedures relating to time and attendance record keeping and hours of duty are contained in IGM Volume V. Employees also will follow INV Headquarters written policy guidelines for entering hours worked into IDMS II and comply with Law Enforcement Availability Pay Act certification requirements.

A. Basic Hours of Work.

- (1) Official and Core Duty Hours – The OIG official duty hours are from 9 a.m. to 5:30 p.m., Monday through Friday. Each office must be open and responsive during these hours. Employees are permitted to start work in the office as early as 6 a.m. and to depart work as early as 3:30 p.m. If a General Schedule 1811 (GS-1811) employee chooses to start work at 6 a.m., the time between 6 a.m. and 7 a.m. will be recorded as Law Enforcement Availability Pay (LEAP). The requirement to work until 3:30 p.m. is consistent with other OIG policies concerning core hours and best suits the mission of the OIG and INV.

Thirty minutes for lunch is always included and may not be substituted for leave or used to shorten the workday. Personnel are not allowed to skip lunch and work an 8-hour day instead of an 8½-hour workday. Field offices may alter the beginning and ending times (for example, flexitour or gliding work schedule) to suit operational needs (for example, 8 a.m. to 4:30 p.m.);

however, the workday for all employees must include the established core hours of 9:30 a.m. to 3:30 p.m.

- (2) **Exceptions to Core Hours** – If operational reasons exist, GS-1811 employees should work LEAP hours prior to 6 a.m. and after 6 p.m. Because assigned workday schedules starting before 6 a.m. and ending after 6 p.m. are subject to night differential pay requirements, employees are not permitted to have their regular workday schedules established outside of these hours.

When an agent must work an earlier, later, or weekend shift to conduct surveillance, conduct an undercover activity, execute a night time search warrant, and so forth, the SAC or assistant special agent in charge (ASAC) may approve in advance an exception to the core hours. Because such shifts may entail payment of night differential or Sunday pay and, therefore, affect the INV budget, all such approvals must have the prior concurrence of the AIGI or the Deputy Assistant Inspector General for Investigations (DAI).

- (3) **Compressed Schedule** – Agent personnel may not work a compressed workweek schedule. However, INV support staff may work a compressed workweek schedule if it does not hinder office operations and is approved in advance by the appropriate field office SAC or INV Headquarters supervisor.
- (4) **Physical Fitness Time** – Time for the OIG’s Fitness Program (Fit time) will be authorized for a maximum of three 1-hour periods per workweek. Fit time is intended to provide opportunities for achieving fitness through activities that develop muscle tone, cardiovascular endurance, strength, and flexibility. Examples of qualifying activities are weight lifting, speed walking, aerobics, martial arts, and swimming. Examples of activities that do not qualify are firearms, golf, bowling, and archery. Fit time is for fitness activity and not for any other purpose. Fit time will not accumulate and will not be used to substitute for leave or to shorten the workday.

Agency needs take precedence over employee participation in the Fitness Program. An employee’s supervisor may grant or deny an individual employee’s participation in the program, based on the demands of the office in which the employee works.

- a. **Times**. Employees are authorized to engage in Fit time activities during regularly scheduled work hours. In addition, employees are allowed to combine the exercise periods with lunch breaks; however, Fit time cannot be claimed while in overtime status and on weekends. Employees are authorized to engage in Fit time activities during LEAP hours if the Fit time is immediately contiguous with the official regular workday and employees depart from and return to their official duty stations following Fit time.

- b. **Locations.** Fit time activity locations are government facilities, commercial health clubs, or other appropriate locations as specifically authorized by an employee's supervisor. Fit time activities are not to be conducted at residences. This prohibition does not apply to employees assigned to domicile locations where the official duty station is the employee's residence.
 - c. **Use of Official Government Vehicle.** Use of an official government vehicle (OGV) to engage in Fit time is authorized, provided the following conditions are met: the employee departs from and returns to his or her official duty station following Fit time; the facility is located within a reasonable distance of the employee's official duty station; and the employee's supervisor approves in advance the employee's use of the OGV for the purpose of driving between the official duty station and the facility.
 - d. **Program Agreement.** Prior to participation in the Fitness Program, employees and their supervisors must sign and date the OIG's Fitness Program Participation Agreement. Employees must sign a program agreement annually to cover the calendar year for which the employee participates in the Fitness Program. The agreement must be retained by the employee's supervisor.
 - e. **Fit Time While on Travel.** While in travel status and provided that all other conditions of this program are met, employees may engage in Fit time without regard to location requirements and time requirements regarding Fit time being taken immediately contiguous with official time.
 - f. **Abuse of the Fitness Program.** Abuse of the Fitness Program constitutes grounds for immediate revocation of the employee's privilege to participate in the Fitness Program and may also result in disciplinary action.
- (5) **Telework.** IGM V-261, "Telework," identifies three types of teleworking: regular, episodic, and single instance. However, because of the nature of INV's mission and work, staff members are only eligible for the episodic and single instance options. (INV requirements are stricter than those in IGM V-261.)
- a. **Episodic Teleworking.** All positions within the INV are eligible for episodic teleworking, which is defined in IGM V-261 as an employee working from home for a specific work assignment or short period of time. Interested staff members must complete OIG Form V-261.1 (Office of the Inspector General Teleworking Agreement Form), which can be found on the OIG Intranet at

(b) (7)(E) and the U.S. Department of Justice Flexible Work Options Request Form at <http://www.usdoj.gov/jmd/ps/doj-fwo.htm>. The Flexible Work Options form requires applicants to identify specifically the work products that will be completed during the teleworking period, recommend how work progress will be monitored, and explain the effect the agreement will have on the office and its staff. Both forms require SAC and INV Headquarters review and approval prior to the commencement of teleworking.

- b. **Single Instance.** All positions within the INV Headquarters are eligible for single instance teleworking, which is defined as an employee working from home for 1 day. Interested staff must complete OIG Form V-261.2 (Office of the Inspector General Teleworking Agreement Form (For Single Instance Teleworking Arrangements)), which can be found on the OIG Intranet at (b) (7)(E). This form requires SAC approval, and a copy of the approved form must be forwarded to the Director, Administrative Support Branch, INV Headquarters.

- B. **Bi-Weekly Time and Activity Reporting.** All nonsupervisory special agents will enter their work hours into the IDMS II "Time Entry Notebook." The Time Entry Notebook is also available for use by nonagent INV personnel.

(b) (7)(E)

- (5) Administrative and Collateral Responsibilities:
- a. Collateral Duties — Enter all assigned collateral duty hours [REDACTED] (b) (7)(E) for example, inventorying equipment and conducting quarterly range qualifications.
 - b. Administration — Report the time spent on administrative and logistical activities, such as preparing noninvestigative reports and studies and attending staff meetings. (b) (7)(E) [REDACTED]
- (6) Liaison — Enter the time spent contacting federal, state, and local law enforcement agencies to encourage cooperation, assistance, and information sharing. Include travel time related to these activities. (b) (7)(E) [REDACTED]
- (7) Fit Time — Enter the time spent working out at a gym, running for example (not to exceed 3 hours per week).
- (8) Training — Enter the time spent in training or developing job-related skills, such as firearms training and attending report writing training classes and legal update training classes.
- (9) In Support of Criminal Investigations/In Support of Other Investigations — Enter supervisory, clerical, and agent time spent on investigative support activities (b) (7)(E) [REDACTED] such as reviewing the SACS report.
- (10) Annual Leave — Enter the number of annual leave hours taken during the 8-hour workday.
- (11) Sick Leave — Enter the number of sick leave hours taken during the 8-hour workday.
- (12) Administrative Leave — Enter the number of hours of preapproved administrative leave taken (such as for jury duty).
- (13) Holiday — Enter the number of hours (usually 8 hours). Even if part of the day was worked as LEAP, 8 hours must still be entered.
- (14) Compensatory Leave — This category applies only to INV personnel who do not receive LEAP. Enter the number of preapproved leave hours taken during the 8-hour workday as compensation for overtime hours previously worked.

- (15) **Other Leave** — This includes Family Leave and Military Leave. Enter the number of preapproved hours taken during the 8-hour workday.
 - (16) **Leave Without Pay (LWOP)** — Enter the number of hours of leave without pay taken during the 8-hour workday (must be preapproved).
 - (17) **AWOL** — Enter the number of hours absent without authorization during the 8-hour workday.
 - (18) **Worker's Compensation** — Enter the number of hours taken that will be charged to the Occupational Workers Compensation Program during the 8-hour workday.
- C. **Total Bi-Weekly Hours.** IDMS II will automatically calculate the totals for each of the above categories of hours worked and for leave taken for each pay period.
- D. **Overtime and Other Pay.** OIG policy and budgetary considerations generally preclude payment of night differential, Sunday pay, holiday pay, or scheduled overtime to employees. All overtime, night differential, Sunday pay, or holiday pay must be fully justified, scheduled in advance, and preapproved by the AIGI. INV employees working such a schedule must provide their hours to their office timekeeper because these items are not included in the IDMS II Time Entry Notebook
- E. **Law Enforcement Availability Pay Act of 1994.** Federal agencies generally pay LEAP to criminal investigators (GS-1811) employees. LEAP provides premium pay to criminal investigators to ensure their availability for unscheduled duty in excess of the 40-hour workweek, based on the needs of the employing agency. The following is OIG policy regarding the payment of LEAP to special agents:
- (1) All GS-1811 criminal investigators will work an average of 2 hours of unscheduled duty per regular workday. The average is calculated over a 12-month period beginning with pay period 01 through pay period 26 and is calculated by dividing the total number of LEAP hours reported for the year by the total number of regular workdays minus total number of excludable days. Excludable days for LEAP are days on which any type of leave exceeds 4 hours per day, days of agency-approved training, and travel days for training. LEAP hours for each pay period can be automatically calculated by IDMS II, based on the agent's entries into the IDMS II Time Entry Notebook.
 - (2) The LEAP Act exempts GS-1811 criminal investigators from the hours of work and overtime pay provisions of the Fair Labor Standards Act (FLSA). When a supervisor places an agent in availability or standby status, it is not considered scheduling the agent for overtime hours as compensated under the scheduled overtime pay provisions of the FLSA.

- (3) The agent has discretion to schedule and work the LEAP hours necessary to accomplish investigative goals and tasks. However, the SAC, ASAC, or DAIGI must approve in advance any LEAP hours not actually worked (for example, standby status).
 - (4) Hours worked qualifying for LEAP include the following:
 - a. Time worked either before or after the agent's normal duty hours of the agent's regular scheduled workday.
 - b. All unscheduled time worked on an agent's nonregular workday (for example, weekend).
 - c. Time worked voluntarily on a holiday.
 - d. Availability time (standby status) must be specified and approved by a SAC or ASAC. For example, if the ASAC directs four agents to remain available at their residences from 8 p.m. until 11 p.m. for possible execution of a search warrant, but the warrant is never executed, the four agents are each entitled to claim 3 hours of LEAP.
 - e. Duty agent time. Duty agents are those agents designated by the SAC or ASAC to be available to respond to and handle emergent investigative activity during nonduty hours. LEAP will only be allowed for time actually worked.
 - (5) Time not qualifying for LEAP includes the following:
 - a. Travel on a nonregular workday to attend a training course.
 - b. Commuting between residence and the office.
 - c. Duty agent time where no actual work is performed.
- F. LEAP Certifications. Samples of the LEAP certification forms are found in Appendix C. Procedures regarding LEAP certification follow:
- (1) Initial — Under the act provisions for LEAP, employees and supervisors are required to make an initial certification that they expect to meet the LEAP eligibility requirements. Employees use OIG Form III-100/2 (Criminal Investigator LEAP Certification). Certifications by agents and ASACs will be reviewed and approved by the respective SAC using OIG Form III-100/1 (Supervisory LEAP Certification). Certifications by SACs will be approved by the DAIGI. The original certifications will be maintained in field office administrative file III-100.

- (2) Annual — All agents, SACs, and ASACs must also sign an annual certification reflecting that they have met and will continue to meet the annual LEAP requirements (OIG Form III-100/4 (Criminal Investigator LEAP Certification) (Annual)). Immediate supervisors must sign OIG Form III-100/3 (Supervisory LEAP Certification) (Annual) certifying that employees under their command met the annual LEAP requirements and are expected to continue to do so. Supervisors will also ensure that semiannual interim LEAP calculations are completed, that any employee who does not meet the required hours is counseled, and that a memorandum of record is prepared and sent to the DAIGI.
- (3) Termination — Termination of availability pay is considered an adverse action under section 7512 (4), title 5, United States Code (5 U.S.C. § 7512 (4)) and part 752, title 5, of the Code of Federal Regulations. Employees have specific rights to appeal adverse actions. SACs must coordinate all LEAP related personnel actions with the DAIGI as well as with the OIG Personnel Office in the OIG Management and Planning Division (M&P) and the OGC. The LEAP Act provides limited exemptions from LEAP requirements in unusual circumstances.

100.7 Annual Home-to-Work Use of an Official Government Vehicle and Driver's License Certification.

- A. Certification for Home-to-Work Use of an Official Government Vehicle. OIG agents and certain supervisors are authorized to use an OGV for official OIG business (b) (7)(E)

Official government vehicles include all vehicles owned, leased, or rented by the OIG. Use of an OGV is subject to the following conditions:

- (1) Each agent/supervisor must have a current, approved OIG Form III-105/4 (Certification for Home-to-Work Use of Official Government Vehicle) on file (b) (7)(E). The annual certification forms will be completed and retained in each field office. The SAC will certify via memorandum to the DAIGI that each potential OGV operator has a current approved OIG Form III-105/4 on file. (See Appendix D for a sample memorandum.) This memorandum certification will be submitted at the same time as the annual LEAP certification (see above) and the annual driver's license certification (paragraph B below), usually in January of each year.
- (2) Annual certification avoids the paperwork burdens associated with daily or weekly written requests to use an OGV. (b) (7)(E)

(b) (7)(E)

(3) Each operator of an official government vehicle, even an occasional operator, must have a valid driver's license issued by the state in which he or she resides.

B. Annual Driver's License Certifications. Each field office SAC must annually certify by memorandum to the DAIGI that all OGV operators under his or her supervision possess valid driver's licenses. (See Appendix D for a sample memorandum.)

(1) The SAC or ASAC must visually inspect the driver's license of each potential OGV operator to assure current validity prior to making the certification.

(2) This certification will be submitted to INV Headquarters with the annual LEAP certification and home-to-work certification, usually in January of each year.

100.8 Official Correspondence. Policies, procedures, styles, and formats relating to official correspondence within the OIG are contained in IGM 1-021. In addition to the guidelines of IGM 1-021, official correspondence emanating from the INV will be handled as follows:

A. Memorandum Format. The memorandum format will be used for all INV correspondence intended for an audience within the DOJ offices, boards, divisions, or bureaus and intended for the signature of an INV official. The original memorandum will be prepared on OIG letterhead. The courtesy and file copies may be prepared on plain copy paper.

B. Letter Format. The letter format will be used for all INV correspondence intended for an audience outside the DOJ offices, boards, divisions, or bureaus and intended for the signature of an INV official and will be prepared on OIG letterhead. The courtesy and file copies may be prepared on tissue or plain copy paper.

100.9 Requests for Review of OIG Files. Information in OIG investigative files may be made available to other agencies only under the following conditions:

A. Law Enforcement Requests. The arrest and disposition of charges against an OIG subject should be a matter of record with the National Crime Information Center (NCIC) if the fingerprints and FBI Form R-84 (Final Disposition Report) were properly submitted, generally making the information readily accessible to other law enforcement agencies. (b) (7)(E)

(b) (7)(E)



- B. Background Investigation Requests. In many of the cases in which the OIG considered allegations to have been substantiated, the subjects of OIG investigations were not prosecuted and may or may not have been the subject of agency disciplinary action. Under all circumstances, the OIG must be diligent in its regard for the privacy and civil rights of DOJ employees and must exercise special care when considering requests for the release of information about subjects of OIG investigations.

(b) (7)(E)

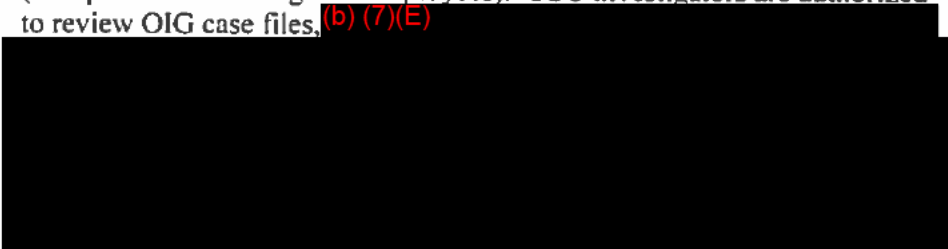


- C. Giglio/Henthorn Requests. Procedures follow for *Giglio* and *Henthorn* requests from federal prosecutors for information regarding prosecution witnesses.
- (1) In *Brady v. Maryland*, 363 U.S. 83 (1963), the Supreme Court held that a criminal defendant is entitled to all exculpatory information in the possession of the prosecution. In *Giglio v. United States*, 405 U.S. 150 (1972), the Court held that any information known by a federal prosecutor, including any impeachment information regarding a prosecution witness, is deemed to be known by all prosecutors serving in the same office. In *Henthorn v. United States*, 991 F.2d 29 (9th Cir. 1991), the Ninth Circuit Court of Appeals ruled that upon request by defense counsel, a prosecutor must provide information from a federal employee witness's personnel file that demonstrates dishonesty or similar conduct.
- a. The DOJ Criminal Division has interpreted "personnel file" to include investigative files.

- b. "Impeachment information" includes any evidence of conduct that undermines a witness's credibility, character, or truthfulness or that demonstrates bias. Failure to provide impeachment information to a defendant may result in charges being dismissed and in the prosecutor being sanctioned by the court.
- (2) Requests received by the OIG under *Giglio* and *Henthorn* may address OIG employees as well as employees of other DOJ components who have been investigated by the OIG. All *Giglio* or *Henthorn* requests shall be promptly transmitted to the OGC for review and response.
 - (3) The DOJ Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Agency Witnesses ("*Giglio* policy") assures that federal prosecutors are provided with all impeachment information regarding government witnesses and protects the privacy interests of a government employee who is called upon to serve as a witness in a criminal case.
 - a. As part of the *Giglio* policy, any government employee (including any OIG employee) who is called upon to serve as an affiant or witness in a criminal prosecution is required to disclose to the federal prosecutor any potential impeachment information about himself or herself.
 - b. In addition, OIG employees are required to advise the OIG (through the OGC) of potential impeachment information that has been disclosed to a federal prosecutor and to update such disclosure to the prosecutor and to the OIG while the case is pending.
 - (4) In addition to requesting potential impeachment information from witnesses themselves, a prosecuting office may request potential impeachment information from an employing or investigative agency (such as the OIG) regarding an employee who is expected to be a witness or affiant in a particular criminal case. In response to such a request, the OIG is obligated to provide:
 - a. Any finding of misconduct that reflects upon the truthfulness or bias of the employee witness.
 - b. Any past or pending criminal charge.
 - c. Any allegation reflecting upon the employee's credibility that is part of an ongoing investigation.

Allegations that are unsubstantiated or have resulted in exoneration will be provided to the prosecuting office only when: the law in a

particular judicial district requires it; the allegation was made by a judge or prosecutor; the allegation received publicity; the prosecutor and the Agency agree that disclosure is appropriate based on exceptional circumstances involving the nature of the case or the role of the Agency witness; or where the Agency deems it otherwise appropriate.

- (5) Disclosure to a prosecuting office does not necessarily mean disclosure to the defendant. Rather, it allows the prosecutor to review the material and determine if the material should be: withheld from the defendant, provided to the defendant, or presented to the court for in camera review to determine if the material should be disclosed or withheld.
- D. Other Special Requests. Special requests from certain agencies for specific purposes will be treated as follows:
- (1) Office of Special Counsel – The Office of Special Counsel (OSC) has statutory authority to investigate whistleblower retaliation complaints (except those involving FBI employees). OSC investigators are authorized to review OIG case files, (b) (7)(E)

 - (2) Financial Records Obtained From a Financial Institution – The Right to Financial Privacy Act (RFPA) (12 U.S.C. §§ 3401-3422) provides that financial records may be obtained from a financial institution by administrative subpoena. Financial records obtained by subpoena under this act may be transferred to another government agency upon a certification by the requesting agency that such records are relevant to a legitimate law enforcement inquiry. Absent a court order to the contrary, the customer must be notified within 14 days after such transfer. Requests for transfer of such records will be coordinated through the OGC to assure compliance with the act. (See also IGM III-230.)
 - (3) Government Accountability Office – A request from the Government Accountability Office (GAO) for OIG investigative information must be in writing, must specifically identify the information sought, and must state the reason for the request. The request will be submitted or transmitted to the OGC. A GAO representative making an oral request for information will be advised that a written request to the OGC is required.

The OGC shall consult with the DAIGI and the field office SAC regarding the status of the investigation and what information, if any, should be provided to GAO. A response to the GAO will be prepared by the OGC with copies sent to the SAC and the DAIGI for their respective office files.

100.10 Congressional Inquiries.

- A. Congressional inquiries will be controlled through the OIG Immediate Office. General policies and procedures for handling congressional inquiries are contained in IGM I-021.
- B. All congressional inquiries coming to the attention of INV personnel will be routed to the Special Operations Branch of INV Headquarters, which in turn will consult with the Immediate Office of OIG regarding how to handle the inquiry and any response.

100.11 Hotline Operations. The OIG maintains a toll-free telephone hotline operated by INV Headquarters.

- A. The hotline number is operational 24 hours a day, 7 days a week. The hotline provides a taped message to callers explaining how to file a complaint either by mail, facsimile, or e-mail.
- B. The OIG Web site contains separate hotline information for filing civil rights and civil liberties complaints, including those related to alleged violations of section 1001 of the Patriot Act.
- C. Hotline complaints will be processed and entered into IDMS II in the same manner as regular complaints. However, the method of receipt field in IDMS II will indicate the code for "hotline."
- D. The SAC, Operations Branch, INV Headquarters, is responsible for providing other specific guidelines for the operation of the hotline to affected personnel.

100.12 Safety and Seatbelt Usage.

- A. Emergency Equipment. All persons operating an OGV will do so in a safe and prudent manner and in compliance with state traffic laws. Emergency lights and sirens (if any) installed in OGVs must meet applicable state requirements. Emergency equipment may only be used when the situation warrants, that is, in a true emergency, and not, for example, because an employee is late for work or for an appointment.
- B. Seatbelts. Any person in a motor vehicle on official OIG business who is occupying a seat that is equipped with a seatbelt must have the seatbelt properly fastened at all times while the vehicle is in motion. This policy applies both to drivers and

passengers, including prisoners or detainees being transported by the OIG. This policy applies to any vehicle used to conduct official business, including rental vehicles. Any malfunctioning seatbelt in an OGV should be repaired or replaced as soon as possible.

100.13 Employee Transfers and Mobility Agreements.

- A. Official Time for Relocating. This policy applies to intra-INV official transfers between geographically dispersed duty stations for both OIG funded Permanent Changes of Station (PCS) relocations and for relocation at employee expense.
- (1) Pre-Move and Post-Move Time – An INV employee permanently relocating from one official duty station to another geographically dispersed official duty station (i.e., more than 50 miles apart) on official transfer orders may receive up to 3 days of official time within 2 weeks before the move and up to 3 additional days within 2 weeks after the move has occurred. This time is for taking care of necessary personal business related to the transfer (for example, pick-up and delivery of household goods and registering personal vehicles in a new state).
 - (2) Official Time While in Transit – If an employee is driving a personally owned vehicle to relocate to the new duty station, they will be allowed one day of official time in transit for each 300 miles driven. If the individual uses air or rail transportation, an amount of time that is reasonable under the circumstances will be approved.
 - (3) Justification – Employees must provide their supervisors with a justification for all requested official time.
 - (4) Allowable Expenses – For PCS moves funded by the OIG, M&P has developed an Employee Relocation Handbook that provides detailed guidance on the entitlements and allowances for relocating employees. The handbook is found on the OIG intranet, under *Documents*. Transferring employees are strongly encouraged to familiarize themselves with the information in this handbook before incurring expenses in connection with an official move.
- B. Mobility Agreements. All newly hired agents and agents transferring to a new official duty station must sign an OIG Form III-100/5 (Mobility Agreement). (See Appendix E.)
- (1) The mobility agreement specifies that the agent agrees to accept reassignment within the OIG at management's discretion for the benefit of the OIG or as part of an OIG Career Mobility Program. Such reassignment would normally occur only after at least 2 years at the current duty station.

- (2) The mobility agreement also contains an addendum stipulating the terms of any mutually agreed upon worksite accommodation.

100.14 Serious Incident Management.

- A. Notification. An employee is required to notify his or her ASAC or first-line supervisor as soon as possible following a serious incident (defined below). The first-line supervisor is required to notify his or her SAC immediately after receiving notification of the serious incident. SACs will then immediately notify the DAIGI of the serious incident.

Following the initial notification of a serious incident, applicable sections of the IGM will be controlling as they apply to further notifications, reports, and other procedures. For example, an employee involved in a shooting will follow the protocols set forth in IGM III-201; an employee detained for questioning in a criminal matter will follow the protocols set forth in IGM I-030.

The timely notification of a serious incident to INV Headquarters allows for appropriate immediate actions to be taken, for example, referring the employee to the Employee Assistance Program, convening a shooting review team, or making notification of the incident to the Oversight and Review Division.

- B. Definition of a Serious Incident. Serious incidents are defined as follows:

- (1) On-duty or work-related incidents involving serious bodily injury requiring medical attention or involving a death;
- (2) Incidents involving the use of a firearm: shooting incidents, accidental discharges, and loss or theft of a firearm (further described in IGM III-201);
- (3) On-duty or work-related incidents involving significant property damage;
- (4) Accidents or incidents of a government-owned or -leased vehicle or a vehicle rented for government use that involve death, serious bodily injury, or substantial property damage;
- (5) Any arrest or any instance in which the employee has been taken into custody, held for investigation, or detailed for questioning, regardless of whether the employee was in a duty or nonduty status at the time of the occurrence;
- (6) Incidents that may result in the immediate attention of the media.

100.15 External Reports. The following is a list of INV recurring administrative/operational reports that are disseminated outside the OIG.

A. Annual Reports.

- (1) **Investigative and Prosecutive Activity Report** – This report is prepared in accordance with Attorney General Guidelines for Statutory Law Enforcement Authority for the Attorney General and is due on November 1 of each year. The report, prepared by the SAC, Investigative Support Branch, INV Headquarters, details the investigative and prosecutive activities of the OIG. The report shall, at minimum, contain information on the number of federal criminal investigations initiated, undercover operations undertaken, and times any type of electronic surveillance was used. Additionally, the report shall provide information on all significant and credible allegations of abuse of the authorities conferred by section 6(e)(1) of the Inspector General Act by Office of the Inspector General investigative agents and what, if any, actions were taken as a result. The names of the agents need not be included in such report.
- (2) **President's Council on Integrity and Efficiency Report** – A report is prepared for the President's Council on Integrity and Efficiency (PCIE) (with ultimate distribution to the President), showing investigative accomplishments during the year. The Director, Administrative Support, INV Headquarters, will prepare this report for submission to M&P. The PCIE will notify the OIG when the report is due.
- (3) **A-123 Year-End Internal Control Report** – The A-123 Year-End Internal Control Report is prepared for M&P (for further distribution to the Attorney General) and summarizes internal control activities performed during the year. IGM V-101 provides OIG policy on internal controls. The Director, Administrative Support, INV Headquarters, will prepare this report for AIGI approval and submit to M&P.
- (4) **Pen Register/Trap and Trace Report** – The Pen Register/Trap and Trace Report is prepared for the DOJ Criminal Division, showing a summary of all pen registers and “Trap and Trace” used during the year. This report is due to the DOJ Criminal Division by September 30 each year. The SAC, Investigative Support, INV Headquarters, will prepare a consolidated report for the AIGI 10 days before the reporting due date each year.
- (5) **Executive Office of U.S. Attorneys Report** – The SAC, Operations Branch, INV Headquarters, is required to submit a monthly report to the Executive Office of U.S. Attorneys (EOUSA), documenting new cases opened involving U.S. Attorney’s Office personnel and providing updated status on pending investigations of such personnel. Field office SACs are required to provide initial notification and monthly updates to the SAC, Operations Branch, INV Headquarters, on all such cases.

- B. Semiannual Reports. The Semiannual Report to Congress is prepared for the Attorney General and Congress to show OIG accomplishments during a 6-month period. The Director, Administrative Support Branch, INV Headquarters, will prepare the INV portion of this report for AIGI approval and submission to M&P. Because specific requirements may vary from year to year, M&P will issue instructions on due dates, formats, and required information.
- (1) Field office SACs will prepare summaries of major cases completed during the previous 6 months and then forward the summaries, by mid-March and mid-September, to the Director, Administrative Support Branch, INV Headquarters. The Director, Administrative Support Branch, will issue instructions on exact due dates, formats, and any other information required.
 - (2) SACs will also ensure that all new allegations received are entered into IDMS II and that all IDMS II screens (for example, judicial, administrative, civil) are updated by midnight each March 31 and September 30. SACs must also submit the monthly Investigative Activity Report (IAR) for March by close of business (COB) on the first business day in April and the September IAR by COB on the first business day in October (Section 100.16).
- C. Quarterly Reports.
- (1) Consensual Monitoring Activities – The report of consensual monitoring activities, which is prepared for the DOJ Criminal Division, reports all OIG consensual monitoring conducted during the quarter. Reports are due to the DOJ Criminal Division on January 31, April 30, July 31, and October 31 each year. The Director, Administrative Support Branch, INV Headquarters, will prepare a consolidated report for the AIGI 10 days before the reporting due date each quarter.
 - (2) A-123 Status Reports – The A-123 Status Reports are prepared for M&P (for further distribution to the Justice Management Division). These reports indicate the status of reviews conducted, corrective actions taken and planned, other significant internal control activities, and any accomplishments. The Director, Administrative Support Branch, INV Headquarters, will prepare the quarterly A-123 Internal Control Reports for AIGI approval by the due dates set by M&P. No status report is required for October 1 each year, as the Year-End Internal Control Report fulfills this requirement.
 - (3) Pen Register – The report of pen registers is prepared for the DOJ Criminal Division to show the results of any pen registers used during the quarter. The reports are due to the Criminal Division by January 31, April 30, July 31, and October 31 each year. The SAC, Investigative Support Branch, INV

Headquarters, will prepare a consolidated report for the AIGI 10 days before the reporting due date each quarter.

- (4) Trap and Trace – The Trap and Trace Report is prepared for the DOJ Criminal Division to show the results of any trap and trace operations conducted during the quarter. The reports are due to the DOJ Criminal Division by January 31, April 30, July 31, and October 31 each year. The SAC, Investigative Support Branch, INV Headquarters, will prepare a consolidated report for the AIGI 10 days before the reporting due date each quarter.

100.16 Internal Reports. The following is a list of INV recurring administrative/operational reports prepared for use within the OIG:

A. Annual Reports.

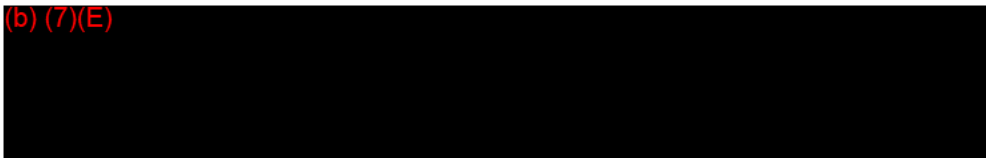
- (1) The Annual Report on Proprietary Operations is prepared for the Inspector General. (See IGM III-250 for further instructions.)
- (2) The Annual Confidential Informant Suitability Review is completed by the SAC who is supervising the handling of the confidential informant (CI) (IGM III-240).
- (3) The Annual Inspection and Inventory of Ballistic Protective Garments, as scheduled by the Investigative Support Branch, is completed by the field office SAC and submitted to the SAC, Investigative Support Branch, INV Headquarters. (See IGM III-201 for further instructions.)
- (4) Annual physical inventory of all OIG-issued firearms assigned to the offices or any weapon authorized for use by the respective field office is forwarded by the field office SAC. The Investigative Support Branch, INV Headquarters, will schedule the inventory and must receive the report through the field office SAC. (See IGM III-201 for further instructions.)

B. Semiannual Reports. The Semiannual Report of Undercover Operations is sent to the Undercover Operations Review Committee by the DAIGI (IGM III-250).

C. Quarterly Reports.

- (1) Review of Undercover Operations – This is completed by the SAC, Investigative Support Branch, INV Headquarters (IGM III-250).

(2) (b) (7)(E)



(b) (7)(E)

- (3) Firearms Training/Qualification – The report of firearms training/qualification is submitted by the field office firearms officer to the AIGI through the field office SAC and the SAC, Investigative Support Branch, INV Headquarters, on a quarterly basis. This report documents the results of the most recent firearms training/qualification periods (IGM III-201).

(4)

(b) (7)(E)

D. Monthly Reports.

- (1) Undercover Operations Progress Report – The Undercover Operations Progress Report is prepared by field office SACs for the SAC, Investigative Support Branch, INV Headquarters, and the DAIGI (IGM III-250).

(2)

(b) (7)(E)

- (3) Investigative Activity Report – The IAR is prepared by each field office SAC for INV Headquarters. Aspects of this report are consolidated and used for various other reports that the INV is required to prepare for dissemination outside the division, including the following: Use of Law Enforcement Authorities, Consensual Monitoring Activities, Trap and Trace Activities, and Semiannual Report to Congress. The IAR covers the use of various investigative techniques, such as consensual monitoring or other (b) (7)(E) polygraphs and (b) (7)(E) SACs must ensure that the reports for March and September are completed in a timely manner and submitted to INV Headquarters by COB of the first business day in April or October, as applicable.
- (4) Priority Case Report – The Priority Case Report is prepared by the SAC, Operations Branch, INV Headquarters, for the Inspector General. The report is based on monthly field office submissions (IGM III-207).

- (5) Standardized Data Collection and Reporting; Activity Based Analysis; Collaborative Management; and Strategic Decision Making (SACS) Report – The Standardized Data Collection and Reporting; Activity Based Analysis; Collaborative Management; and Strategic Decision Making (SACS) Report is prepared by INV Headquarters and disseminated to the field for use as a case management tool (IGM III-207).
- (6) Budget (Travel and Supply) Reconciliation – For the Executive Office for U.S. Attorneys Report, the SAC, Operations Branch, INV Headquarters, submits a monthly report to EOUSA, documenting new cases opened involving U.S. Attorney’s Office personnel and providing updated status on pending investigations of such personnel. Field office SACs are required to provide initial notification and monthly updates to the SAC, Operations Branch, INV Headquarters, on all such cases.

E. Weekly Reports.

- (1) AG Weekly Report – This report is initially prepared by each field office. Its purpose is to highlight major significant developments (such as an arrest, plea, or conviction) in significant cases that may be of interest to the Attorney General. Each field office must submit this report to the Director, Administrative Support Branch, INV Headquarters, for review and consolidation into a division-wide report by close of business each Friday. The AG Weekly Report is then submitted to the Inspector General for further review, consolidation, and submission to the Attorney General (IGM III-232).
- (2) Weekly Report to the FBI on New FBI Investigations Opened by the OIG – This report is prepared by the SAC, Special Operations Branch, INV Headquarters, for submission to a counterpart in the FBI Office of Professional Responsibility, under a mutual reporting agreement with the FBI. For this reason, field office SACs must notify the SAC, Special Operations Branch, before opening any FBI investigation.

F. Miscellaneous Reports.

- (1) Closeout Review of Proprietary Operations – This report is completed by the SAC, Investigative Support Branch, INV Headquarters, and OIG auditors within 90 days after closing down a proprietary operation (IGM III-250).
- (2) Review of Undercover Activity – This report is completed by ASACs 30 days after termination of undercover activity (IGM III-250).
- (3) (b) (7)(E)

(b) (7)(E)

- (4) Loss of Weapon – This report is forwarded to the ASAC (with copies to the security officer and the Security Programs Manager) not later than close of business of the first working day following the loss or theft of an OIG issued or authorized firearm (IGM III-201).

- (5) Critical Incidents and Firearms Policy Review Committee – Within 2 weeks after the committee convenes (based on receipt of an investigative report regarding any critical incident), the committee will issue a final report to the Inspector General (IGM III-201).

APPENDIX A

**Sample Box Marking and Addressing for Investigative Case Files
Sent to Records Storage Facility**

COMPLAINTS CLASSIFIED AS "I" (INVESTIGATION)

At the End of the File Retention Period.

(b) (7)(E)



b. Destruction date (10 years from the inactive date as described in Subsection 100.5D.)

(b) (7)(E)



APPENDIX B

Inventory Transmittal

(OIG Form III-100/6)

This form may be reproduced

U.S. Department of Justice
Office of the Inspector General

Inventory Transmittal

From:	DOJ/OIG/INVESTIGATIONS- HQ/WFO 1425 New York Ave, NW Suite 7100 Washington, D.C. 20005	Account #	(b) (7)(E)
		Page	of
To:	(b) (7)(E)	Date	

Remarks:

Box #	Description (File Numbers and File Name)	Date Closed	Destruction Date (10 years after inactive date)

Shipped	
Date:	Signature and Title

APPENDIX C

Supervisory LEAP Certification (Initial)
(OIG Form III-100/1)

Criminal Investigator LEAP Certification (Initial)
(OIG Form III-100/2)

Supervisory LEAP Certification (Annual)
(OIG Form III-100/3)

Criminal Investigator LEAP Certification (Annual)
(OIG Form III-100/4)

Sample Memoranda and Calculation Steps

INITIAL LEAP CERTIFICATION

This certifies that, over the course of the next 12 months, I expect the criminal investigators on the attached list [attach OIG Form III-100/2], who are officially assigned to positions properly classified in the GS-1811 Criminal Investigator Series under the Position Classification Standards issued by the U.S. Office of Personnel Management to average at least 2 hours of unscheduled duty per regular workday.

_____/_____
(Signature/Date)

Special Agent in Charge _____ Field Office

Attachment

CRIMINAL INVESTIGATOR LEAP CERTIFICATION

INITIAL LEAP CERTIFICATION

The undersigned criminal investigator understands that, as a condition of receiving availability pay under 5 U.S.C. 5545a, I will be required, over the course of the next 12 months, to perform (or be available for) at least an average of 2 hours of unscheduled duty per regular workday. I understand that failing to average at least 2 hours of unscheduled duty per regular workday may result in an overpayment.

_____/_____
(Special Agent Signature/Date)

ANNUAL SUPERVISORY LEAP CERTIFICATION

This certifies that, over the course of the past 12 months, the criminal investigators on the attached list [attach OIG Form III-100/4], who were officially assigned to positions properly classified in the GS-1811 Criminal Investigator Series under the Position Classification Standards issued by the U.S. Office of Personnel Management averaged at least 2 hours of unscheduled duty per regular workday.

Over the course of the next 12 months, I expect the criminal investigators on the attached list to continue to average at least 2 hours of unscheduled duty per regular workday.

_____/_____
(Signature/Date)

Special Agent in Charge _____ Field Office

Attachment

CRIMINAL INVESTIGATOR LEAP CERTIFICATION

ANNUAL LEAP CERTIFICATION

This certifies that, over the course of the past 12 months, the undersigned criminal investigators averaged at least 2 hours of unscheduled duty per regular workday. We understand that failing to average at least 2 hours of unscheduled duty per regular workday may result in an overpayment.

We understand that as a condition of continuing to receive availability pay under 5 U.S.C. 5545a, we will be required, over the course of the next 12 months, to average at least 2 hours of unscheduled duty per regular workday.

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

_____/_____/_____
(Signature/Date/LEAP Hr Avg.)

DATE

MEMORANDUM

TO: INSERT NAME
 Deputy Assistant Inspector General
 For Investigations

FROM: INSERT NAME
 Special Agent in Charge
 INSERT NAME of Field Office

SUBJECT: Interim LEAP Review

Reference is made to OIG policy concerning Law Enforcement Availability Pay Act of 1994 interim semiannual reviews.

Please be advised that all agents from the _____ Field Office are currently meeting the average hours requirements as set forth in the act. Any exceptions are noted below.

DATE:

MEMORANDUM

TO: INSERT NAME
 Deputy Assistant Inspector General
 For Investigations

FROM: INSERT NAME
 Special Agent in Charge
 INSERT NAME of Field Office

SUBJECT: Annual LEAP Certification

Reference is made to OIG policy as outlined in IGM III-100, concerning the Law Enforcement Availability Pay Act of 1994 (LEAP) annual certification.

Please be advised that the annual hours worked calculation for LEAP certification has been conducted and all agents from the _____ Field Office have met the hourly requirement as set forth in the Act. Any exceptions are noted in attached memorandum.

INSERT DATE

MEMORANDUM FOR INSERT NAME
Deputy Assistant Inspector General
For Investigations

FROM: INSERT NAME
Special Agent in Charge
INSERT FIELD OFFICE NAME

SUBJECT: LEAP Exceptions

Please be advised that for the period _____ through _____ the person(s) listed below have fallen below the average LEAP hours requirement of 2 hours of unscheduled duty per regular workday as set forth in the Inspector General Manual, Volume III, Chapter 100, "General Administration," Subsection 100.6(E), "Law Enforcement Availability Pay Act of 1994."

<u>Name</u>	<u>Total LEAP Hours</u>	<u>Average LEAP Hours per Day</u>
-------------	-------------------------	-----------------------------------

- 1.
- 2.

APPENDIX D

**Annual OGV Home-to-Work and
Driver's License Certifications**

U.S. Department of Justice
Office of the Inspector General

INSERT DATE

MEMORANDUM FOR INSERT NAME
Deputy Assistant Inspector General
For Investigations

FROM: INSERT NAME
Special Agent in Charge
INSERT FIELD OFFICE NAME

SUBJECT: Annual (b) (7)(E) Certification

In accordance with IGM Volume III, Chapter 105, "Use of Official Government Vehicles: OIG Policy, Procedures, and Fleet Management," Section 105.7, "OGV Home-to-Work Use of OGVs," please be advised that all special agents from the OIG, Investigations Division, _____ Field Office have completed OIG Form III-105/4 (Certification for Home-to-Work Use of Official Government Vehicle) for calendar year 20__.

In addition, I certify that for each of these special agents, (b) (7)(E) use is necessary for the safe and efficient performance of criminal law enforcement duties as set forth in IGM III-105 and in the Attorney General's Authorized (b) (7)(E) Action Plan for the Office of the Inspector General.

U.S. Department of Justice
Office of the Inspector General

INSERT DATE

MEMORANDUM FOR INSERT NAME
Deputy Assistant Inspector General
For Investigations

FROM: INSERT NAME
Special Agent in Charge
INSERT FIELD OFFICE NAME

SUBJECT: Annual Valid Driver's License Certification

In accordance with the IGM, Volume V, Chapter 410, "Fleet Management," Section 410.7, "Use," please be advised that all employees from the OIG, Investigations Division, _____ Field Office who use government-owned or -leased vehicles possess a valid driver's license issued by the state in which he/she resides. Any exceptions are noted and explained below.

APPENDIX E

OIG Special Agent Mobility Agreement
(OIG Form III-100/5)

This agreement between the Office of the Inspector General (OIG) and _____,
Special Agent, sets forth the terms and conditions for geographic relocations of OIG Special Agents.

As a Special Agent, you agree to accept reassignment within the OIG and within the United States determined solely in management's discretion for the benefit of the OIG or as part of an OIG Career Mobility Program. Allowable expenses associated with such transfer(s) will be paid by the OIG. Except for extraordinary circumstances, you will not be required to move within two years of your initial appointment, nor will you be requested to move within two years of a previous relocation.

ADDENDUM FOR WORKSITE ACCOMMODATION

On occasion, the OIG and an agent may agree on a mutually desirable worksite accommodation allowing the agent to work at a location other than a Field or Area Office. Such accommodation may include work from a city remote from the Field or Area Office to which the agent is assigned. Agents participating in such accommodations agree not to assert any claim against the OIG in connection with a decision by the OIG to end the accommodation. Such a decision will not be considered a reassignment under the above Mobility Agreement. The OIG is not obligated to pay any expenses associated with a move from the accommodation worksite to the agent's former Field or Area Office, regardless of distance.

Special Agent

Date

Assistant Inspector General
Investigations Division
Office of the Inspector General

Date

APPENDIX F

Definitions of Terms in the Prison Rape Elimination Act

DEFINITIONS OF TERMS IN THE PRISON RAPE ELIMINATION ACT

The definition of *sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer* includes any of the following acts, with or without consent of the inmate, detainee, or resident:

- (1) contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) contact between the mouth and the penis, vulva, or anus;
- (3) contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (4) penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (5) any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (6) any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1)-(5);
- (7) any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of an inmate, detainee, or resident, and
- (8) voyeurism by a staff member, contractor, or volunteer.

Voyeurism by a staff member, contractor, or volunteer means an invasion of privacy of an inmate, detainee, or resident by staff for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring an inmate to expose his or her buttocks, genitals, or breasts; or taking images of all or part of an inmate's naked body or of an inmate performing bodily functions.

Sexual harassment in a confinement setting includes:

- (1) repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- (2) repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 100
General Administration
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was originally issued on May 19, 1997, and was rewritten on April 23, 2007, to reflect updates and changes in policies, laws, and guidelines.

This chapter revision includes an inserted revised policy, approved by the Inspector General or his Designee, issued July 9, 2014:

This policy addition is in conformance with the Prison Rape Elimination Act (PREA), Public Law 108-79, which was passed unanimously by Congress in 2003, and AG Order No. RIN 1105-AB34, as codified in the Code of Federal Regulations (C.F.R.), Title 28, Part 115, on May 16, 2012. (See also www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf.)

100.5F: Adds guidance concerning processing and investigation of allegations of sexual abuse in confinement settings (Policy Memorandum FY 14-POL-03).

Appendix F: Adds Definitions of Terms in the Prison Rape Elimination Act (Policy Memorandum FY 14-POL-03).



U.S. Department of Justice

Office of the Inspector General

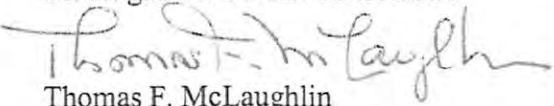
Washington, D.C. 20530

October 24, 2006

POLICY MEMORANDUM
2007- POL-06
III - 100

MEMORANDUM

TO: Investigations Division Personnel

FROM: 
Thomas F. McLaughlin
Assistant Inspector General
For Investigations

SUBJECT: Office Security Procedures Enhancements

This Investigations Division (INV) policy memorandum is being issued in order to provide guidance to INV personnel regarding enhancements to office security procedures. This memorandum contains both mandatory and suggested procedures. Procedures containing the directions “will” or “must” are prescriptive and require mandatory implementation. Procedures containing the direction “should” are permissive and are suggestions for implementation. However, INV personnel should implement the suggested procedure unless there is a compelling reason not to do so.

The proposed office security procedures and policies contained within the document are addressed under the following headings:

- Establishment of Written Procedures
- Procedures for Allowing Subjects and Witness into OIG Space
- Physical Security and Access to OIG Space

The requirements prescribed in this memorandum are effective immediately and apply to all INV personnel.

Establishment of Written Procedures

(b) (7)(E)



- Be provided to the SAC of Investigative Support Branch (ISB).

(b) (7)(E)



- Be provided to the SAC of the ISB.

(b) (7)(E)



- Must be provided to the SAC of the ISB.

Procedures for Allowing Subjects and Witnesses Into OIG Space

(b) (7)(E)



Posting of Signs

Each office will post a sign

(b) (7)(E)

A large black rectangular redaction box covers the majority of the text in this section, starting below the word 'sign' and extending to the right and down.

Scheduling of Interviews

(b) (7)(E)

A large black rectangular redaction box covers the entire text in this section, starting below the section header and extending across the width of the page.

Admittance of Witnesses Into OIG Space

The following procedures will be followed for the admittance of witnesses and their attorneys and union representatives into OIG space:

(b) (7)(E)

A very large black rectangular redaction box covers the entire text in this section, starting below the introductory sentence and extending almost to the bottom of the page.

(b) (7)(E)

A large black rectangular redaction box covering the top portion of the page.

Admittance of Subjects Into OIG Space

The following procedures will be followed for the admittance of subjects and their attorneys and union representatives into OIG space:

(b) (7)(E)

A large black rectangular redaction box covering the middle portion of the page.

Rescheduling of Canceled Interviews

(b) (7)(E)

A large black rectangular redaction box covering the bottom portion of the page.

Physical Security and Access to OIG Space

Each office must ensure the security of the office [REDACTED]
(b) (7)(E)

(b) (7)(E)

Office Locks and Keys

- Each office will be equipped with [REDACTED] locks for all high security doors.
(b) (7)(E)

- Only OIG personnel will be issued keys for the high security locks.
(b) (7)(E)

Escorting of Non-OIG Personnel

- Non-OIG personnel (visitors, cleaning personnel, etc.) will be escorted while in OIG space.

If you have any questions regarding this policy memorandum, please contact SAC Willie Haynes, Investigative Support Branch, at (202) 616-4741.



U.S. Department of Justice

Office of the Inspector General

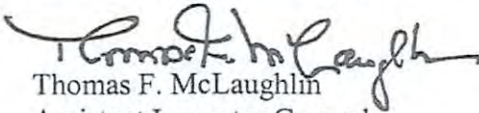
Washington, D.C. 20530

January 24, 2008

POLICY MEMORANDUM
2008- POL-01
III - 100

MEMORANDUM

TO: Investigations Division Personnel

FROM: 
Thomas F. McLaughlin
Assistant Inspector General
For Investigations

SUBJECT: Standards for Safeguarding Sensitive But Unclassified
Information

This Investigations Division (INV) policy memorandum is being issued in order to provide guidance on INV's implementation of Inspector General Manual (IGM), Vol. I, Chapter 222 entitled "Standards for Safeguarding Sensitive But Unclassified Information." This chapter was issued October 31, 2007, and is attached to this policy memorandum as a reference. All INV personnel are required to read and become familiar with this policy memorandum and Chapter 222.

INV Specific Requirements

IGM I Chapter 222 contains specific and general guidelines for protecting Sensitive But Unclassified (SBU) information. In some instances, the chapter requires that the divisions provide specific guidance to their employees on how to comply with the requirements of the chapter. As a result, INV employees must comply with the guidance below in addition to the requirements prescribed in Chapter 222.

Responsibilities § 222.4C

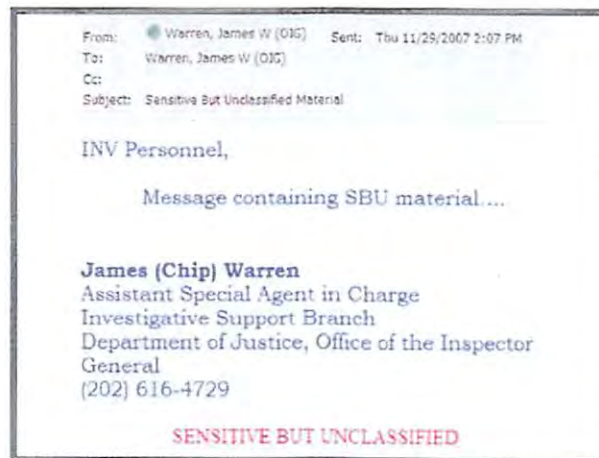
Each field SAC must prepare written procedures by March 1, 2008, to ensure information originating under their supervision meets the minimum protection levels established in Chapter 222. SACs will provide a copy of the procedures to SAC Willie Haynes, Investigative Support Branch, and disseminate the procedures to their employees.

Definitions § 222.5

This section provides the definition for SBU and provides examples of SBU. One of the examples of SBU references “specified” informant and witness information and “specified” investigative material. The INV Division considers all informant, witness, and investigative material to be SBU. Therefore, all such material will be safeguarded in accordance with this chapter.

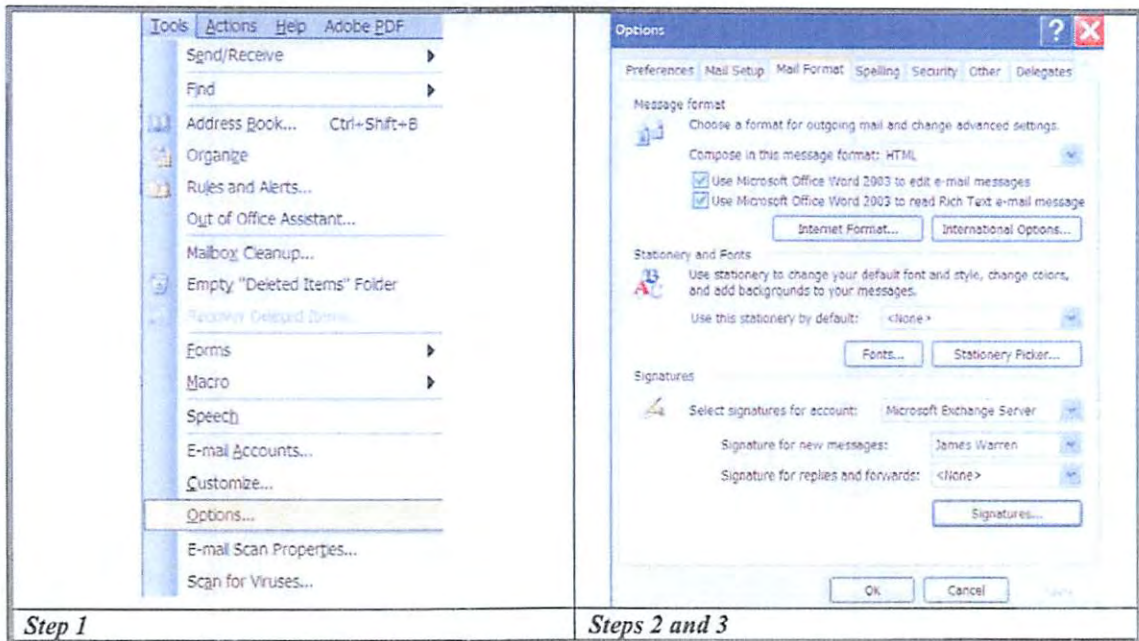
Identification and Markings § 222.6A

This section provides guidance on the proper marking of SBU material. In addition to the requirements listed in this section, all INV email messages containing SBU material will be marked “SENSITIVE BUT UNCLASSIFIED” in the signature section of the body of the email as illustrated below.



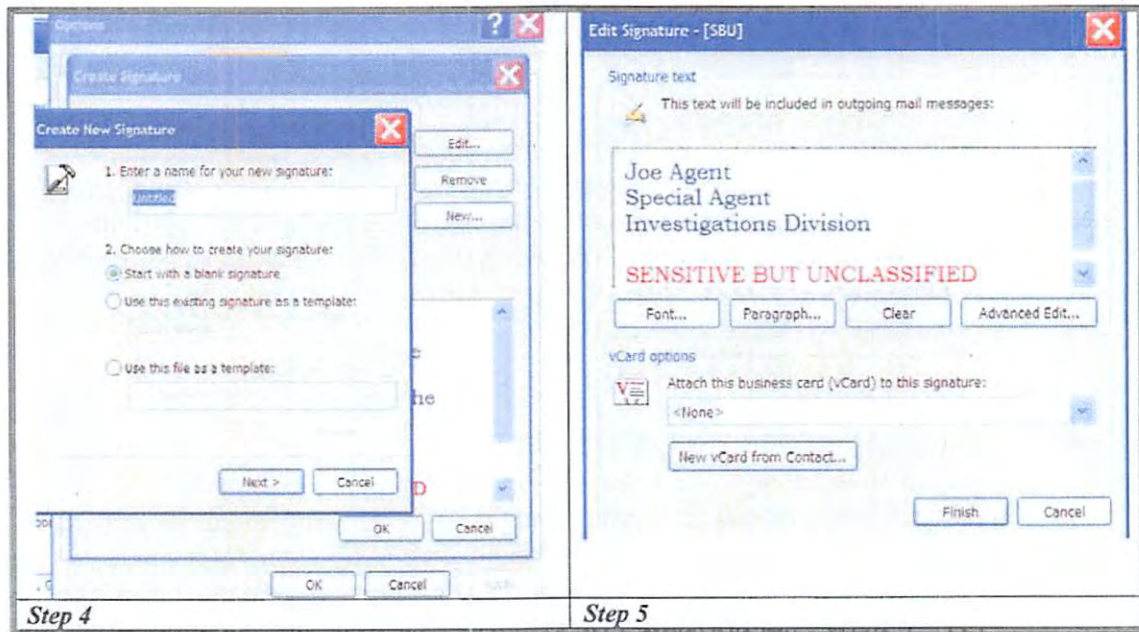
In order to set email messages to automatically include the “Sensitive But Unclassified” marking in the signature section of the email message, follow the instructions below:

1. Under “Tools” in Outlook, select “Options”
2. Under “Options,” select “Mail Format” tab
3. Under “Mail Format” tab, select “Signatures”
4. Under “Signatures,” select “New,” and then type in the name of the signature (or edit a signature if one has already been created)
5. Type in the information wanted in the signature block including the “SENSITIVE BUT UNCLASSIFIED” and then select “Finish”
6. On the “Mail Format” tab, choose the signature from the drop-down next to “Signature for new messages” and “Signature for replies and forwards”



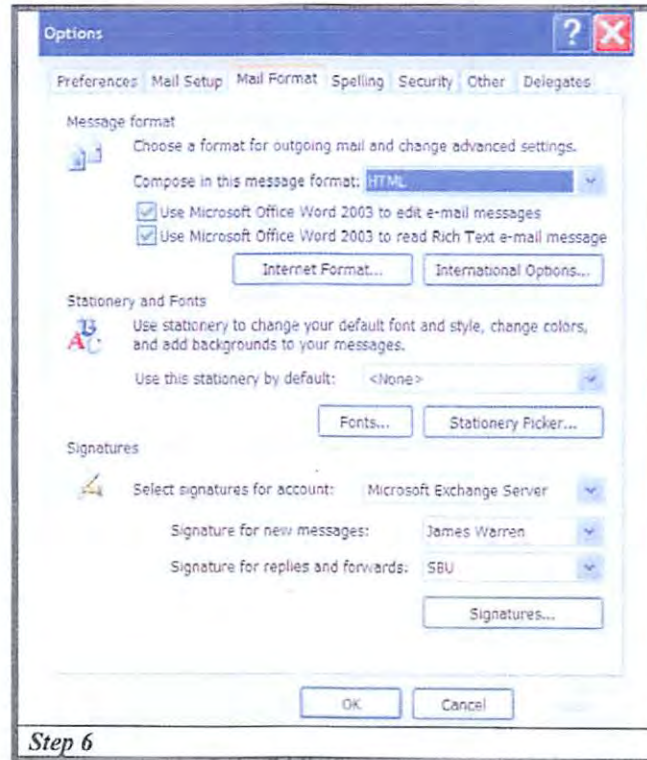
Step 1

Steps 2 and 3



Step 4

Step 5



In addition, the blue ROI and AROI cover sheets will be marked with Sensitive But Unclassified in red capital letters (Times New Roman 16 font) centered in the footer section at the bottom of the sheet (shown below). Two electronic templates will be forwarded to the field offices so that the SBU advisement can be added to already printed coversheets and so that new cover sheets can be printed.

SENSITIVE BUT UNCLASSIFIED

SBU Taken Out of an OIG Facility § 222.6B(3)

Employees are reminded to remove from the office only the minimum amount of SBU material needed to accomplish the task at hand. In addition, employees must ensure that laptop computers have encryption software installed and that the password is not noted on the laptop or in the laptop carrying case. Finally, electronic files containing SBU, including PII, must be transmitted only on approved encrypted storage devices, such as an OIG flash drive, or on an encrypted OIG laptop computer.

Prior to removing any electronic databases or files containing a significant amount of SBU material, employees must receive approval from their supervisors and provide their supervisors with the file name and location of the file on the network server. This requirement is prescribed so that in the event that the file is lost or stolen a

vulnerability assessment can be performed. IDMS and the NFC database are examples of electronic databases containing significant amounts of SBU material.

In the event that other SBU material is removed from the office and then lost or stolen, INV personnel are responsible for being able to provide their supervisors with a list of the SBU that was lost or stolen so as to mitigate the potential harm caused by the loss. To ensure that personnel are able to comply with this inventory requirement, INV personnel must implement the following procedures relevant to the type of SBU removed from OIG space:

Computers Containing SBU Taken Out of OIG Office Space

Use the following process in order to make specific folders and files containing SBU available on a computer outside of OIG office space. Following these steps will ensure that an inventory of documents can be produced at a later date. The laptop computer must be connected to the network (docked) before starting this process.

1. Maintain all official files on the H:/ drive server. Check to make sure that there are not any official files on the C:/ drive.
2. Right Click on the Start Menu and Select Explore.
3. Click on Tools, Folder Options, Off-Line Files Tab.
4. Check the first 3 boxes (Enable Offline Files, Synchronize All Offline Files When Logging on, Synchronize All Offline Files before Logging off).
5. Click the "Apply" Button, then "Ok."
6. Remain in Explore and Right click on any H drive server files that are to be available off-line (i.e. a folder named "Current Cases" or "Travel Vouchers") and Select Make Available Off-line. The first time you do this it will probably launch into a Wizard. If it does not open a wizard, skip to Step # 8.
7. If the Wizard opens, have it Auto Synch during log on and off. Uncheck the "reminder" box. Do not create a short cut to offline files on the desktop. Be sure to make subfolders available off-line.
8. The first time the computer synchs (depending on the number of files being synched) it will take a minute or two to create off-line copies. A small white box with two blue arrows will appear in the left corner of each folder/file that will be available off-line. If for some reason the synching process creates an icon on the desktop, do not use the icon.
9. When a folder or file no longer needs to be available off-line, go to the H:/ drive while connected to the network, right click the folder/file and deselect the "Make Available Offline" option.

Access to the offline files is the same as the access to them on-line, i.e. still click on the H:/ drive and open the files in the same manner as if your computer was connected to the network.

This process makes an exact duplicate of your selected H:/ drive folders and files on your laptop when disconnected from the network. Whenever logging on or off the

network this procedure ensures they files are synched. It is a seamless process to the user.

Any problems with this process should be resolved by contacting the Help Desk.

If an employee is unable to complete the above process for any reason, such as at a domicile office, the employee must manually save on the H:/ drive each electronic file containing SBU that is to be removed from OIG office space. The files are to be stored on the H:/ drive in a folder entitled "SBU Files Inventory." The employee must complete the procedure prior to removing the electronic files.

OIG Issued Flash Drives

A duplicate of all of the electronic files contained on the flash drive must be retained on the H:/ drive in a folder entitled "Flash Drive Inventory." In the event that the flash drive is lost or stolen, employees or management will be able to retrieve the files from the H:/ drive.

Hard Copy Documents and Other Items Containing SBU

Employees will prepare an inventory of SBU documents and other SBU items to be removed from the office prior to departing OIG office space. This inventory is to be completed either on the spreadsheet that will be sent via email to all INV personnel upon implementation of this policy, or in some other appropriate manner. An example of the spreadsheet is attached to this policy memorandum.

If you have any questions regarding this policy memorandum, please contact SAC Willie Haynes, Investigative Support Branch, at (202) 616-4741.

Attachments

Type of Media (Paper, CD, Flash Drive, Computer, etc...)	Description of SBU Material
MOI (hard copy)	case no. 2007-001234; dated 11/12/07; interviewee Bob Smith
MOI (hard copy)	case no. 2007-001234; dated 11/15/07; interviewee Ted Williams
Autotrax report	Bob Smith; ssn 123-45-6789
Bank Records (hard copies)	Ted Williams account numbers (Bank of America 123404999; Wachovia 1233299879)

**Office of the Inspector General
United States Department of Justice**

REPORT OF INVESTIGATION

Case Number: _____

Date: _____

Report Provided to:



THIS REPORT CONTAINS SENSITIVE LAW ENFORCEMENT MATERIAL. IT MAY NOT BE LOANED OUTSIDE YOUR AGENCY AND, EXCEPT IN CONNECTION WITH OFFICIAL AGENCY ACTION, NO PORTION OF THE REPORT MAY BE COPIED OR DISTRIBUTED WITHOUT THE KNOWLEDGE AND CONSENT OF THE INSPECTOR GENERAL.

SENSITIVE BUT UNCLASSIFIED

222.1 Policy. The Office of the Inspector General (OIG) is entrusted with handling sensitive but unclassified (SBU) information. This information must be appropriately safeguarded to comply with applicable laws and regulations and to protect individual rights or critical operations of the OIG or the Department of Justice (DOJ). It is the policy of the OIG to comply with these laws and regulations and provide adequate protection to safeguard SBU information.

Guidance for the processing and handling of classified information and data is addressed separately in Inspector General Manual (IGM), I-220, Document Security.

222.2 Reference. These procedures are in accordance with DOJ Order Nos. 2600.2C, 2600.4, 2610.2A, 2620.5A, 2620.7, 2640.1, and 2640.2E, and the DOJ Security Programs Operating Manual.

222.3 Scope. This chapter applies to all OIG employees and contractors. This chapter provides specific guidance on the processing and handling of SBU information and data and should be read in conjunction with IGM I-220, which provides guidance specific to the processing and handling of classified information and data.

222.4 Responsibilities.

A. The Inspector General (IG) is responsible for:

- (1) specifying through this directive the categories or types of information that originate in the OIG and are designated as SBU;
- (2) identifying those subordinate officials who have authority to determine if information originating under their supervision or cognizance qualifies as SBU or requires protection in excess of the minimum levels established in this directive, and the officials so designated are responsible for ensuring that personnel under their direction are aware how to properly handle, store, and transmit these special designated categories and all categories of information considered SBU.

B. The Security Programs Manager (SPM) has the responsibilities described in DOJ Order 2600.2C and also is responsible for:

- (1) ensuring the safekeeping of SBU material in the OIG;
- (2) overseeing OIG employee and contractor compliance with information security requirements;
- (3) ensuring that OIG contracts adequately incorporate and comply with all information security requirements;

- (4) providing guidance to OIG personnel in information security matters;
 - (5) ensuring that adequate security equipment and storage devices are available; and
 - (6) ensuring that adequate security measures and procedures are implemented to protect SBU information.
- C. Office Heads are the highest level official in each office location. They are responsible for:
- (1) overseeing compliance with information security requirements at the facility;
 - (2) developing office-specific guidance to ensure information originating under their supervision meets the minimum protection levels established in this directive; and
 - (3) designating a primary and alternate Security Officer for the facility.
- D. Security Officers are responsible for protecting SBU information in the facility and maintaining communications with the SPM for local security operations.
- E. Employees and contractors are responsible for the protection and storage of SBU information and materials in their custody.

222.5 Definitions.

- A. Sensitive information is any information of which the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of OIG, DOJ, or federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that is not classified as national security information.
- B. The categories or types of sensitive information within the OIG include, but are not limited to, SBU, Limited Official Use (LOU), For Official Use Only (FOUO), and Law Enforcement Sensitive (LES), hereinafter referred to collectively as SBU. In no case should information be designated as SBU or any other sensitivity category to conceal inefficiency, misdeeds, or mismanagement.
- C. The following categories are provided for illustrative purposes only as examples of the types of OIG information considered SBU:

- (1) Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, such as their full name, social security number, date and place of birth, mother's maiden name, biometric records, and any other personal information that is linked or linkable to a specific individual. Some personal information is not generally considered PII because many people share the same trait, including first or last name, country, state, or city of residence, age, gender, race, name of school and workplace, and grades, salary, or job position;
- (2) specified informant and witness information;
- (3) grand jury information;
- (4) specified investigative material;
- (5) tax information;
- (6) information that could be sold for profit;
- (7) reports that disclose security vulnerabilities;
- (8) information that could result in physical risk to individuals; and
- (9) company proprietary information.

222.6 Procedures.

A. Identification and Markings.

- (1) OIG material that contains information the IG or his designee has determined is SBU must be appropriately identified to ensure that all persons having access to the information outside of the OIG's control are aware of the protection requirement.
- (2) The identification of sensitive information may be accomplished by written instructions or a marking of SBU or another category of sensitive information in one of the following manners:
 - a. on the first page of the material;
 - b. a notation in a covering memorandum;
 - c. use of a cover sheet;

- d. use of a sticker on computer media; or
- e. any other method authorized by the IG.

(3) The purpose of identifying SBU information is to ensure that all recipients of the material not familiar with OIG or DOJ policies are aware that the information requires protection.

B. Storage and Transmission.

(1) General.

- a. Personnel who have custody of material designated as SBU shall exercise care to ensure that the information is not available to individuals who have no legitimate business need for access to the information.
- b. At a minimum, unauthorized individuals must not be able to enter areas unobserved and have visual access to SBU information.

(b) (7)(E)

- d. The sensitivity of some SBU, including but not limited to tax information and grand jury information, may require a higher level of protection. (b) (7)(E)
- Questions regarding information protected under the references listed in Section 222.2 of this directive should be directed to the SPM. Questions regarding categories of information originating within the division described in Section 222.4.A.(2) of this directive should be directed to the appropriate designated official in your division.

(2) Information Technology Systems.

- a. Non-OIG computers, including personally-owned computers, shall not be used to store or process OIG or DOJ data with one exception:

(b) (7)(E)

- b. OIG data are prohibited from being stored or processed on any networked computer outside of the OIG's IGNITE network,

with one exception: (b) (7)(E)



- (3) SBU Taken Out of an OIG Facility.
- a. Electronic files containing SBU, including PII, must be transmitted only on approved encrypted storage devices or on an encrypted OIG laptop computer.
 - b. OIG employees and contractors should transport only the minimum amount of SBU information necessary for their duties. OIG Divisions may develop additional division-specific guidance for removing SBU information from an OIG or DOJ facility. This guidance may require that an inventory of specified types of SBU files being transported be conducted and provided to the supervisor prior to removal from the OIG facility.
 - c. Prior to removing certain SBU information specified by OIG Divisions from an OIG facility, an employee must obtain the supervisor's approval.

(b) (7)(E)



(4) Custody of SBU While on Official Travel

(b) (7)(E)



- b. SBU must not be reviewed in public places where people without a “need to know” can inadvertently view either documents or information on an OIG laptop computer.

(b) (7)(E)



(b) (7)(E)



C. Access and Dissemination.

(1) Access.

- a. No OIG personnel or non-OIG personnel, including but not limited to contractors, may be given access to SBU information unless that

person has the appropriate background investigation and a need-to-know for the performance of official duties.

- b. Access to SBU information should be maintained at the minimum number of persons consistent with operational requirements.
- c. OIG employees, including students and contractors, will be considered eligible for access to SBU information after a favorable personnel security determination has been made by the Director, Justice Management Division, Security and Emergency Planning Staff in accordance with Executive Order 10450 and IGM I-201, Personnel Security.

(2) Dissemination.

- a. When disseminating hard copy documents that contain SBU, including but not limited to PII, OIG employees must protect the information from unauthorized use, disclosure, and visual access.

(b) (7)(E)



b.

- c. SBU must not be left openly visible in common work areas that regularly receive visitors, such as reception areas, conference rooms, and mailrooms.

D. Destruction and Reuse.

(1) Document Destruction.

- a. SBU documents must be destroyed by shredding or other methods such as burning or pulping.

There is no minimum size requirement for the residue of shredded SBU documents, as there is with National Security Information, so

all single-cut or cross-cut shredders are sufficient for destruction of these documents.

(b) (7)(E)



(2) IT Systems and Media Destruction.

- a. IT systems that have processed, stored, or transmitted SBU or classified information shall not be released from the OIG's control until the equipment is sanitized by degaussing and removal of all memory components. This requirement includes equipment donated to schools and other organizations.

OIG contractors are responsible for providing the COTR with a written certification that all DOJ data has been removed prior to releasing equipment from the contractor's control.

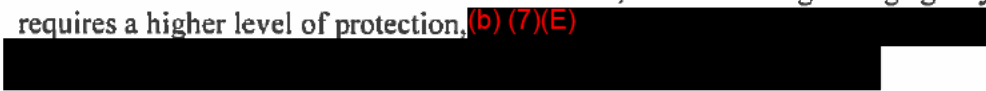
- b. OIG IT equipment under maintenance warranty contracts shall include stipulations that equipment removed from OIG offices shall be sanitized before removal.
- c. When no longer usable, diskettes, tape cartridges, ribbons, and other similar items used to process SBU and classified information shall be destroyed by being overwritten with nonsensitive data, degaussed, shredded, or incinerated, whichever method is available, appropriate, and cost effective.
- d. When no longer usable, compact disks used to process SBU shall be destroyed by shredding, using a CD destroyer, or physically breaking the disk into pieces.

(3) IT Removable Media Reuse.

When no longer required for mission or project completion, IT storage media that will be re-utilized by another person within the OIG shall be overwritten with software and protected consistent with the data sensitivity level at which they were previously used.

E. SBU Collected and Provided by Other Agencies.

Sensitive materials and data provided by other agencies must be maintained in accordance with Section 222.6B of this directive, unless the originating agency requires a higher level of protection. (b) (7)(E)



F. Incident Reporting and Handling Requirements.

(1) Reporting the Loss or Theft of SBU.

- a. OIG employees and contractors must report the loss or theft of sensitive materials and data, whether in document or electronic format, to their supervisor or COTR, or designated higher level official, as soon as the loss or theft is determined.
- b. The supervisor or COTR and office head must collect the facts surrounding the loss and the extent of any potential damage from the loss and report the incident immediately to the SPM and Information Systems Security Officer (ISSO) and provide periodic updates as additional information is developed.
- c. The SPM and ISSO must report the loss of SBU and the extent of any potential damage from the loss to the DOJ Computer Emergency Readiness Team (DOJCERT) within one hour after they receive notification of the loss or theft and provide periodic updates as additional information is developed. DOJCERT will report DOJ incident information, common vulnerabilities, and threats to OMB and US-CERT when required.

(2) Handling Requirements.

In addition to reporting to DOJCERT, the SPM and affected Division must assess the potential damage that may be caused by the loss of SBU and make a determination if it is also necessary to notify originating agencies or affected individuals of the possible security breach.

A security breach includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where persons other than authorized users and for an other than authorized purpose have access or potential access to SBU, including PII, whether documents or electronic data.

- (3) Compliance.
 - a. Compliance with this policy will be enforced through sanctions commensurate with the level of infraction if it is determined that employee negligence was a factor in the loss or breach.
 - b. An appropriate disciplinary action may be imposed depending on the severity of the violation.



Washington, D.C. 20530

October 30, 2006

POLICY MEMORANDUM
2007- POL-07
III - 100

MEMORANDUM

TO: Investigations Division Personnel

FROM: 
Thomas F. McLaughlin
Assistant Inspector General
For Investigations

SUBJECT: Traumatic Incidents: Reporting Requirements and
Management

This Investigations Division (INV) policy memorandum is being issued in order to provide guidance to INV personnel in responding to and dealing with traumatic incidents.

This memorandum incorporates new guidelines; elements of the Inspector General Manual (IGM), Volume III, Chapter 201 – Firearms; and Policy Memorandum 2006-POL-04 (reporting requirement for serious incident management). Although this memorandum focuses primarily on shooting incidents, these guidelines may be applied following any incident that has resulted in death or serious bodily injury. These guidelines are intended to reduce the chances that INV personnel will develop or suffer from post-traumatic stress disorder following a traumatic incident.

The requirements prescribed in this memorandum are effective immediately and apply to all INV personnel.

Definitions

Agent-Involved Shooting Incident: A shooting incident that occurs in the line-of-duty that causes death or serious bodily injury to any person.

Traumatic Incident: An incident that causes stress sufficient to overwhelm the coping skills of an individual or group. The event may have the potential to interfere with the

ability to function either at the scene or thereafter. If the incident is extreme in nature, it may serve as a starting point for post-traumatic stress disorder.

Post-Traumatic Stress Disorder: An anxiety disorder that can result from exposure to short-term severe stress or from the long-term buildup of repetitive and prolonged milder stress. It may result from an exposure to a traumatic event.

Serious Incident: An incident that meets one or more of the following criteria:

- 1) Occurs on-duty or is otherwise work-related and results in death, serious bodily injury; and/or significant property damage.
- 2) Involves the use of a firearm: shooting incidents, accidental discharges, and loss or theft of a firearm;
- 3) Involves a government-owned or -leased vehicle or a vehicle rented for government use and results in death, serious injury, and/or significant property damage;
- 4) Involves an arrest or instance in which an employee has been taken into custody, held for investigation, or detained for questioning, regardless of whether the underlying conduct occurred on or off-duty ;
- 5) May result in immediate media attention.

Reporting Requirements for Serious Incidents

Notwithstanding other directives and policies, an employee is required to notify his or her first-line supervisor as soon as possible following a serious incident. Some serious incidents, such as shooting incidents, are ***traumatic incidents*** and may require further actions as provided for below. Upon receiving any such notification, the first-line supervisor must immediately notify the appropriate Special Agent in Charge (SAC). The SAC must immediately notify the Deputy Assistant Inspector General for Investigations (DAIGI).

Following the initial notification of a serious incident, employees will comply with the section of the IGM applicable to the particular type of incident that has occurred. For example, for agent-involved shootings, employees will follow the protocols set forth in IGM Vol. III, Chapter 201 and in this policy, while an employee detained for questioning in a criminal matter will follow the protocols set forth in IGM Vol. I, Chapter 030.

The timely notification of a serious incident to INV Headquarters allows for appropriate immediate actions to be taken. Some immediate actions that might follow the notification are actions such as referring the employee to the Employee Assistance

Program (EAP), convening a shooting review team, and making notification of the incident to the Oversight and Review Division.

Shooting Incident Procedures

Field Supervisor Responsibilities

An OIG supervisor will be dispatched to the scene of an agent-involved shooting or other location to which the involved agent(s) has been taken. He or she will assume primary responsibility for caring for involved OIG personnel. Supportive face-to-face communication can help alleviate fear on the part of the involved agent(s) regarding the agency's reaction to the incident. The supervisor does not have to comment on the incident; what is important is to show concern and empathy for the agent.

The supervisor should take the following actions:

- 1) Make appropriate notifications to the Assistant Inspector General for Investigations.
- 2) Assist in making appropriate arrangements for necessary medical treatment.
- 3) Adapt his or her actions accordingly because the handling of a shooting investigation by local authorities will vary greatly.
- 4) Arrange for the agent(s) involved in the shooting to leave the area as soon as possible, in cooperation with the authorities investigating the shooting.
- 5) Have the agent(s) taken to a quiet area away from the immediate scene of the incident during any period where the involved agent(s) is required to remain on the scene but has no immediate duties to fulfill. A counselor or other supportive agent should remain with the involved agent but should not discuss details of the incident with the involved agent(s).
- 6) Keep the following in mind when meeting with the involved agent(s):
 - The agent(s) should not be provided caffeine or other stimulants or depressants unless administered by medical personnel.
 - The supervisor should ask minimal, preliminary questions about the incident but should not press for details. He or she should also advise the agent(s) that a more detailed debriefing will be conducted at a later time. Before undergoing a detailed interview, the agent(s) should have some recovery time in a secure setting shielded from the press and onlookers.
 - The supervisor should encourage the involved agent(s) to notify his or her family about the incident as soon as possible.

- The supervisor should discuss with the agent(s) any standard investigations that he or she can expect to occur.
- The agent(s) should be advised that he or she may wish to seek legal counsel.
- The agent(s) should be cautioned not to discuss the incident with anyone except a personal or agency attorney, association representative, or agency investigator, until the conclusion of the preliminary investigation.

(b) (7)(E)



- 8) Ensure that if an agent has been killed or injured, the agent's family is contacted by an agent personally known to the family. If no agent personally knows the family, then a manager (SAC or ASAC) will notify the family. This agent (or manager) will personally notify the family and arrange for them to be transported to the hospital or other suitable location. Field office personnel should also be notified of the agent's condition so that they may respond to inquiries from family members who may call the field office. It is particularly important that family notification occur before press and or media accounts appear. The supervisor may request assistance from the Employee Assistance Program (EAP) in notifying the family.
- 9) Handle the agent and all involved personnel in a manner that acknowledges the stress caused by the incident.
- 10) Make a referral to the appropriate U.S. Attorney's office if there is a possible violation of title 18 U.S.C. § 111 (assaulting, resisting, or impeding certain

officers or employees) or § 1114 (protection of officers and employees of the United States).

INV Headquarters Responsibilities

- 1) The AIGI should notify the Inspector General of all available facts. The Office of General Counsel and the Management & Planning Division (M&P) may also be advised of particular matters associated with the incident.
- 2) INV Headquarters personnel will contact the Justice Management Division (JMD) EAP to arrange for appropriate support. Peer support teams will be provided by and coordinated through JMD and the EAP. These peer support teams may be composed of individuals from the FBI, the DEA, or other components as appropriate.
- 3) An INV Headquarters manager will be sent to the incident site as appropriate.
- 4) INV Headquarters will ensure that the affected field office has sufficient managerial and administrative support.
- 5) INV Headquarters will notify INV employees of the incident as appropriate.
- 6) The AIGI or his or her designee should coordinate with the Inspector General and field supervisor regarding any media responses concerning a shooting incident.

M&P Responsibilities – Information and Reference for INV Managers

If the shooting has resulted in the **death** of an agent, the AIGI or his or her designee will notify the head of Human Resources, M&P. A benefits specialist will be assigned to perform the following duties/functions:

- The benefits specialist is responsible for reviewing the employee's Official Personnel Folder (OPF) to determine beneficiaries.
- After review of the OPF, the Benefits Specialist will prepare a letter to the spouse of the deceased employee for the human resources officer's signature, detailing all benefits that the survivor is entitled to. This letter should be sent within 1 week of the employee's death.
- The benefits specialist will then prepare a variety of documents and perform a variety of duties, to include:
 - Preparing an estimate for retirement (CSRS/FERS) death benefits for the survivor and children, if there are any.
 - Preparing an estimate for life insurance.

- Preparing forms for a termination of health benefits for the deceased and for a change in health benefits for the survivor and children, if appropriate, and sending with the death benefit forms to the Office of Personnel Management (OPM) and Office of Workers Compensation Programs (OWCP).
- Contacting the Thrift Board to determine the deceased's TSP account balance as of the date of death. The benefits specialist processes the necessary forms for death benefits. A copy of the marriage license and a copy of the certified death certificate are required.
- Completing an SF 52 (Request for Personnel Action), indicating the nature of action as death. The SF 52 should be processed as quickly as possible. It is the driving force for all benefits being processed for the deceased employee. No benefits can be paid from National Finance Center without the processing of the SF 52. The SF 52 is processed by the human resources assistant.
- Estimating the unpaid compensation of the last salary check and the lump sum annual leave payment. A certified copy of the death certificate is required. The unpaid compensation is processed by the human resources assistant.
- Processing the form for gratuity benefits, requesting \$10,000. Of this amount, \$1,000 is paid for funeral expenses and administrative costs by the OWPC. This process is done through the National Finance Center.
- Processing the necessary forms for OWCP benefits. A copy of the certified death certificate, marriage certificate, and an autopsy report is required. These materials are sent to the appropriate OWCP District Office.
- Processing the necessary forms for death benefits for CSRS/FERS benefits. If the survivor elects OWCP in lieu of CSRS/FERS, OPM should be informed of the election. A copy of the certified death certificate, marriage license, and a copy of Certified Summary of Federal Service is required.
- Processing a request for benefits under the Public Safety Officers Benefits Program. A copy of the certified death certificate, marriage license, investigation report and autopsy report is required.

- Preparing a memorandum for the human resources officer's signature, requesting a memorial certificate. This process is coordinated with the JMD staff.
- Transmitting forms to the appropriate agency: OPM, DOL, TSP, FEGLI, NFC, etc. These forms should be processed within 30 days of the death of the employee.

Post Shooting Incident Procedures

- 1) Involved personnel may be relieved of active investigative duties pending an evaluation, but remain available for administrative duties. Alternatively, involved employees may be placed on administrative leave for some period of time in order to allow them time to process the emotional impact of the event. Three days is usually sufficient, although more or less may be appropriate. M&P will provide specific advice concerning administrative leave as appropriate for the situation.
- 2) Any agent involved in a shooting is required to participate in a "Traumatic Incident Stress Debriefing" (TISD). The TISD will be conducted by a knowledgeable mental health professional. The debriefing should take place as soon after the shooting as practical, generally within 24 to 72 hours. Fitness for duty and any need for follow-up sessions will be determined by the mental health professional.
- 3) A supervisor should brief the affected field office regarding the incident to assist in keeping rumors in check. The AIGI (or another individual specifically designated) will release a brief account of the incident via electronic mail to all offices.
- 4) In conjunction with OIG Headquarters, administrative or other investigations related to the incident will be completed as expeditiously as possible. The agent will be advised of the outcome of all investigations.
- 5) All personnel involved in a shooting incident should be advised that they are not permitted to speak with the news media about the incident.
- 6) The OIG public affairs officer (or designated representative) will address inquiries from the media and will release a statement, if appropriate, pertaining to the incident. The interests of the agent will be considered prior to making any media releases. If a field supervisor is authorized to make a statement to the news media, he or she should not vary from the approved statement.

Injured Agent Procedures

If an agent is seriously injured on duty and expected to remain hospitalized, the following actions should be taken:

- 1) Assign a senior agent to the hospital. The agent will act as a liaison to coordinate the following:
 - Security and privacy of the injured agent;
 - Inquiries from OIG and other law enforcement officers;
 - Media inquiries;
 - Visiting hours with office personnel.
- 2) Ensure additional items of evidence are properly secured by the hospital, e.g., clothing. When in doubt treat items as evidence.
- 3) Keep OIG management and office personnel apprised of the condition of the agent.
- 4) Assist the agent in coordinating with M&P to obtain various benefits. An M&P benefits specialist will provide assistance and guidance in this area.

Management Follow-up

- 1) Post-traumatic stress disorders may not be evident immediately, or the agent may attempt to hide the problem. Each supervisor is responsible for monitoring the behavior of office personnel for symptoms of post-traumatic stress disorder. The following are some symptoms of which supervisors should be aware:
 - *Re-experiencing the trauma*: flashbacks, nightmares, intrusive memories and exaggerated emotional and/or physical reactions to triggers that remind the person of the trauma.
 - *Emotional numbing*: feeling detached, lack of emotions (especially positive ones), and loss of interest in activities.
 - *Avoidance*: avoiding activities, people, or places that remind the person of the trauma.
 - *Increased arousal*: difficulty sleeping and concentrating, irritability, hyper-vigilance (being on guard), and exaggerated startle response.

- 2) A supervisor may require an agent to seek assistance or counseling from a mental health professional. This action may be taken upon a reasonable belief that stress may be disrupting the agent's job performance or ability to carry a firearm.

If you have any questions regarding this policy memorandum, please contact SAC Willie Haynes, Investigative Support Branch, at (202) 616-4741.



U.S. Department of Justice

Office of the Inspector General

Washington, D.C. 20530

April 7, 2008

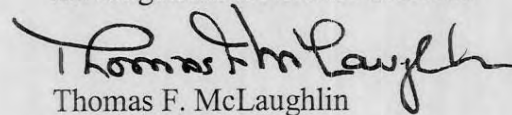
POLICY MEMORANDUM
2008- POL-03
III - 100

MEMORANDUM

TO:

Investigations Division Personnel

FROM:


Thomas F. McLaughlin
Assistant Inspector General
For Investigations

SUBJECT:

Standards for Safeguarding Sensitive But Unclassified
Information – *Superseding Policy*

This Investigations Division (INV) policy memorandum is being issued in order to provide *superseding guidance* to policy memorandum 2008-POL-01, “Standards for Safeguarding Sensitive But Unclassified Information,” dated January 24, 2008. This policy memorandum provides the guidance in the same manner as it will appear in the Inspector General Manual; it supplements IGM Vol. I, Chapter 222 also entitled “Standards for Safeguarding Sensitive But Unclassified Information.” This memorandum is effective immediately.

Policy

100.20 INV Standards for Safeguarding Sensitive But Unclassified Information.
IGM I Chapter 222 contains specific and general guidelines for protecting Sensitive But Unclassified (SBU) information. In some instances, the chapter requires that the divisions provide specific guidance to their employees on how to comply with the requirements of the chapter. INV employees must comply with the guidance below in addition to the requirements prescribed in Chapter 222.


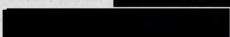
- A. Definitions. IGM I § 222.5 provides the definition for SBU and provides examples of SBU. One of the examples of SBU references “specified” informant and witness information and “specified” investigative material. The INV Division considers all informant,

witness, and investigative material to be SBU. Therefore, all such material will be safeguarded in accordance with this chapter.

- B. Identifications and Markings. IGM I § 222.6A provides guidance on the proper marking of SBU material. In addition to the requirements listed in this section INV personnel will comply with the following:
- (1) All INV e-mail messages containing SBU material will be marked "SENSITIVE BUT UNCLASSIFIED" in the signature section of the body of the email.
 - (2) ROI and AROI cover sheets will be marked with Sensitive But Unclassified in red capital letters (Times New Roman 16 font) centered in the footer section at the bottom of the sheet.
- C. SBU Taken Out of an OIG Facility. In relation to IGM I § 222.6B(3), employees are reminded to remove from the office only the minimum amount of SBU material needed to accomplish the task at hand. In addition, employees must ensure that laptop computers have encryption software installed and that the password is not noted on the laptop or in the laptop carrying case. Electronic files containing SBU, including PII, must be transmitted only on approved encrypted storage devices, such as an OIG flash drive, or on an encrypted OIG laptop computer.
- (1) Prior to removing any electronic databases or files containing a significant amount of SBU material, employees must receive approval from their supervisors and provide their supervisors with the file name and location of the file on the network server. This requirement is prescribed so that in the event that the file is lost or stolen a vulnerability assessment can be performed. IDMS and the National Finance Center database are examples of electronic databases containing significant amounts of SBU material.
 - (2) INV personnel are responsible for being able to provide their supervisors with a list of any SBU that is lost or stolen so as to mitigate the potential harm caused by the loss. INV personnel must implement the following procedures relevant to the type of SBU removed from OIG space:
 - a. *Computers Containing SBU Taken Out of OIG Office Space.* Employees must ensure that computers removed from OIG space have been configured so as to ensure that an inventory of documents can be produced at a later date. (b) (7)(E)

(b) (7)(E)



- b. *OIG Issued Flash Drives.* A duplicate of all of the electronic files contained on the flash drive must be retained (b) (7)(E) 
 Employees may only use OIG issued flash drives which are encrypted.
- c. *Hard Copy Documents and Other Items Containing SBU.* Employees should be prepared to provide management with a description of any hardcopy document or other item containing SBU removed from the office and subsequently lost. Employees may consider preparing an inventory of SBU documents and other SBU items to be removed from the office prior to departing OIG office space. Employees may use any appropriate method in order to be able to provide the necessary information in the event of loss.

If you have any questions regarding this policy memorandum, please contact SAC Willie Haynes, Investigative Support Branch, at (202) 616-4741.



December 20, 2010

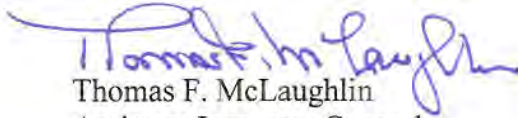
POLICY MEMORANDUM

FY11-POL-02

III – 100

MEMORANDUM

TO: Investigations Division Personnel

FROM: 
Thomas F. McLaughlin
Assistant Inspector General
For Investigations

SUBJECT: Law Enforcement Availability Pay Policy Changes

This Investigations Division (INV) policy memorandum changes the narrative in IGM III § 100.6. This policy is effective immediately.

Background

As requested by the Special Agent Advisory Committee, INV has reviewed the policy on Law Enforcement Availability Pay (LEAP) calculation and the definition of an excludable day.

In defining an excludable day, the following sources were reviewed: 5 C.F.R. §§ 550.181-185; Office of Personnel Management Availability Pay Fact Sheet; Department of Justice (DOJ) Guidance: Availability Pay, Chapter 2-1; DOJ Time and Attendance Handbook; and other documents related to LEAP.

This policy change allows agents to claim an excludable day for purposes of LEAP calculation if they travel for more than 4 hours to and from a Temporary Duty Station. This policy change also allows agents to claim LEAP hours on an excludable day when the total hours for the day (excludable and worked) exceed 8 hours. Changes in the policy are bolded and italicized.

Policy100.6 Time and Attendance. NO CHANGE

- A. Basic Hours of Work. NO CHANGE
- B. Bi-Weekly Time and Activity Reporting. NO CHANGE
- C. Total Bi-Weekly Hours. NO CHANGE
- D. Overtime and Other Pay. NO CHANGE
- E. Law Enforcement Availability Pay Act of 1994. Federal agencies generally pay LEAP to criminal investigator (GS-1811) employees. LEAP provides premium pay to criminal investigators to ensure their availability for unscheduled duty in excess of the 40-hour workweek, based on the needs of the employing agency. The following is OIG policy regarding the payment of LEAP to special agents:
 - (1) All GS-1811 criminal investigators will work an average of 2.0 hours of unscheduled duty per regular workday. The average is calculated over a 12-month period beginning with pay period 01 through pay period 26 and is calculated by dividing the total number of LEAP hours reported for the year by the total number of regular workdays minus the total number of excludable days. ***The following guidelines apply to the determination of excludable days and the calculation of the yearly LEAP average:***
 - a. An excludable day is defined as any regular workday that ***includes occurrences of more than 4 hours of any of the following activities: training, time spent in travel status traveling to and from a Temporary Duty Location, approved leave (for example, annual, sick, and administrative), and other excused absences such as Leave Without Pay.***
 - b. ***A criminal investigator may combine excludable day eligibility requirements in a single workday in order to accumulate more than 4 hours of excludable time (for example, 3 hours of training and 2 hours of annual leave).***
 - c. ***A criminal investigator may claim LEAP hours on the same day as an excludable day provided the LEAP hours are in addition to a combination of 8 hours of excludable time and work time (for example, 6 hours of travel and 5***

hours of actual work would result in 3 hours of LEAP for the day as well as an excludable day).

(2) NO CHANGE

(3) NO CHANGE

(4) NO CHANGE

(5) NO CHANGE

F. LEAP Certifications. NO CHANGE

If you have any questions regarding this policy memorandum, please contact SAC Roger Williams, Investigative Support Branch, INV Headquarters, at (202) 616-4770.

- 200.1 Policy. This chapter establishes investigative and ethical standards for the Investigations Division (INV), Office of the Inspector General (OIG). The OIG shall conduct all investigations as an independent fact-finding organization, with an understanding of the critical and sensitive nature of the task. Professional care will be employed when conducting and reporting investigations. Investigations will be objective, thorough, and completed in a timely manner.
- 200.2 Reference. This chapter is issued under the authority contained in the Inspector General Act of 1978; the title 5 appendix of the United States Code, as amended; Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority, dated December 8, 2003; part 45 of title 28 of the Code of Federal Regulations (28 C.F.R. 45); and 28 C.F.R. 16B.
- 200.3 Scope. The provisions of this chapter will apply to all employees of the INV.
- 200.4 Procedures. The sections of this chapter prescribe procedures regarding specific ethics and investigative standards.
- 200.5 Quality Standards for Investigators. Due to the critical and sensitive nature of their positions, all OIG agents must possess the knowledge, skills, and abilities necessary to fulfill their responsibilities. Agents must have knowledge of the theories, principles, practices, and techniques of investigation. They will also have the requisite skills to apply such knowledge to the type of investigation being conducted. These skills are attained through education, training, and experience.
- A. Knowledge. Agents must have a good working knowledge of Department of Justice (DOJ) organizations, programs, activities, and functions and their interrelations with the private sector. Agents must know the applicable laws, rules, and regulations, such as the U.S. Constitution, the U.S. criminal code (title 18 of the United States Code) (including elements of crimes), the Federal Rules of Evidence, the Federal Rules of Criminal Procedure, and other pertinent statutes, such as the Privacy Act, Freedom of Information Act, and the Whistleblower Protection Act.
- B. Abilities. Agents must be able to exercise tact, initiative, ingenuity, resourcefulness, and sound judgment in collecting and analyzing facts, evidence, and other relevant data. Agents must also possess the ability to use sound deductive reasoning and make effective oral and written reports.

Agents must be able to safely and effectively carry out their law enforcement powers, including carrying firearms, applying for and executing search warrants, serving subpoenas, and making arrests. (See the Inspector General Manual (IGM), Volume III, Chapter 201 (III-201), III-230, and III-232.)

- C. Skills. Proper training is required in order to develop the special knowledge and skills necessary to conduct OIG investigations; therefore, agents are required to successfully complete formal entry-level basic training, formal in-service training, and on-the-job training. Every agent should possess the following skills:
- (1) Obtaining information from people.
 - (2) Obtaining and preparing signed sworn statements.
 - (3) Analyzing and understanding documentary evidence, such as bank records, phone records, and accounting records.
 - (4) Understanding witness confidentiality requirements and “whistleblower” concepts.
 - (5) Evaluating evidence; making sound, objective assessments and observations; and where appropriate, making constructive recommendations.
 - (6) Effectively using computer equipment, software, and related systems to support the investigative process.
 - (7) Selecting and using appropriate and authorized special investigative equipment, such as miniature body transmitters and video cameras.
 - (8) Delivering clear, concise, accurate, and factual summaries of investigations, both orally and in writing.

200.6 Planning, Execution, Reporting, and Information Management. These four critical standards in planning, execution, reporting, and information management must be addressed in order for any investigative effort to be successful:

- A. Planning. Investigative priorities shall be established, and specific case objectives shall be developed to ensure that individual investigative tasks are performed efficiently and effectively. (See also IGM III-207.)
- B. Execution. Investigations shall be initiated and conducted in a timely, efficient, thorough, and legal manner. OIG agents are independent fact gatherers and shall not allow conjecture, unsubstantiated opinion, or bias to affect work assignments. Agents have a duty to be equally receptive to both exculpatory evidence and evidence that is incriminating. Interviews of subjects and witnesses shall be conducted in an effective and perceptive manner. Agents will collect evidence, both physical and testimonial, in such a way as to ensure that all relevant material is obtained, that the chain of custody is preserved, and that the evidence is properly admissible in any subsequent judicial or administrative proceeding.

- C. Reporting. Investigative reports must cover all relevant aspects of the investigation, correctly and succinctly describe the facts revealed and evidence obtained, remain free from personal bias, and be understandable to the prosecutor or lay reader. In pursuing this standard, agents will adhere to the following general guidelines:
- (1) Written Reports. The facts must be set forth in a logical manner and in such a way as to facilitate reader comprehension, even if the reader is unfamiliar with DOJ operations. Potential readers of OIG reports include Assistant United States Attorneys (U.S. Attorneys), chairs of congressional committees, agency heads, administrative law judges, and arbitrators.
 - a. The principles of good report writing must be followed. The report writer's skills will be evaluated based on report completeness, accuracy, clarity, brevity, cohesiveness, and impartiality. The investigative report is frequently the only reflection of the nature and quality of the work accomplished by the OIG that is seen by Assistant U.S. Attorneys, agency heads, or others.
 - b. A high quality investigative report addresses each allegation received and should require little correcting or rewriting. It is submitted in a timely manner, following, as closely as possible, the completion of the investigation.
 - c. Investigative reports will reflect what the investigation accomplished. Accomplishments include, for example, any fines, savings, recoveries, administrative actions, indictments, convictions, or procedural reform recommendations resulting from the investigation.
 - d. Agents will use standardized reporting formats established by the OIG consistent with applicable laws and regulations.
 - e. Detailed investigative report writing and formatting guidelines can be found in IGM III-207 and III-208.
 - (2) Oral Reports. When presenting cases to prosecutors or testifying in any official proceeding, the agent's appearance, demeanor, and conduct should reflect favorably upon the OIG. There must be adequate preparation for testimony. Facts are to be presented in an unbiased, truthful, complete, and convincing manner. Answers shall be brief, yet responsive. An agent serving as a witness should avoid being argumentative when under cross-examination.
- D. Information Management. An effective information management system creates institutional memory and enhances the OIG's ability to fulfill its mandate of detection and prevention of waste, fraud, and abuse. The results of investigations

will be stored in a manner that facilitates retrieval and cross-referencing of information in a timely, efficient, and effective fashion. (Also see IGM III-100, III-205, and III-207.)

- 200.7 Ethics and Standards of Conduct. OIG INV employees must possess and maintain the highest standards of conduct and ethics, including unimpeachable honesty and integrity. INV employees must become familiar with and comply with the general standards of conduct for federal government employees as promulgated in federal statutes (such as section 201 of title 18 of the United States Code (18 U.S.C. § 201) and 18 U.S.C. § 242), Executive Order (EO) 12674 (as amended by EO 12731), the DOJ Ethics Handbook, and IGM I-030. In addition, the following ethical guidelines apply to all law enforcement personnel in the INV:
- A. Contact With Represented Persons. Bar rules applicable to DOJ attorneys place certain limits on their ability to contact parties who are represented by counsel, concerning the subject of that representation. The actions of agents working at the direction of such attorneys may be imputed to the attorneys. The majority of courts have held that preindictment, noncustodial contacts do not violate the anticontact rule. Nevertheless, because local rules and practices may differ from jurisdiction to jurisdiction, agents should consult with the assigned prosecutor regarding the applicable rules in a particular case. If an agent has questions about this issue in connection with an administrative case or a criminal matter to which no prosecutor is assigned, the agent should contact the OIG Office of General Counsel (OGC).
 - B. Contact With Complainants, Victims, Witnesses, Informants, or Subjects. When conducting an investigation, INV employees must not fraternize with complainants, victims, witnesses, informants, or subjects involved in that investigation in any manner that creates partiality or the appearance of partiality. Prohibited activities include, but are not limited to, accepting meals, using vehicles, using copying services or other office facilities, and socializing during or after duty hours, if not directly related to the investigation.
 - C. Contact With Jurors. While a particular jury is seated, contact with grand or petit jurors will be limited to official testimony situations only.
 - D. Ethics Training. All INV personnel will complete the annual ethics training provided by the OIG OGC.
- 200.8 Professionalism. Supervisors and agents must always be aware that they are representatives of the DOJ. Professional demeanor and attire are two key elements of this role.
- A. The maintenance of a calm, business-like attitude, even under adverse situations, is essential.

- B. Proper professional attire will be worn, except when specific work assignments dictate otherwise.
- C. Grooming must be appropriate and professional.
- D. When other than business attire is required for assignments being conducted undercover or if weather conditions dictate, the wearing of other than business attire in the office may be approved by the special agent in charge (SAC).

200.9 Due Professional Care. All INV personnel will follow the due professional care standards established by the President's Council on Integrity and Efficiency in conducting investigations and in preparing related reports.

- A. Objectivity and Impartiality. Agents must be equally receptive to both exculpatory evidence and evidence that is incriminating. All investigations, as well as the resulting reports, must be free from bias or prejudice.
 - (1) All investigations must be conducted in a fair and equitable manner, with the perseverance necessary to determine the facts.
 - (2) Evidence must be gathered and reported in an unbiased and independent manner in an effort to determine the validity of an allegation or to resolve an issue.
- B. Thoroughness. All investigations must be conducted in a diligent manner. Reasonable steps will be taken to ensure that pertinent issues are sufficiently resolved and that all appropriate criminal, civil, contractual, or administrative remedies are considered.
- C. Legal Requirements. Investigations will be initiated, conducted, and reported in accordance with:
 - (1) All applicable laws, rules, and regulations.
 - (2) Guidelines of DOJ and other prosecutive authorities.
 - (3) Internal OIG policies and procedures.
 - (4) The rights and privacy of all those involved.
- D. Appropriate Techniques. Specific methods and techniques used to conduct each investigation must be appropriate for the circumstances and objectives.
- E. Timeliness. All OIG investigations will be conducted and reported with due diligence and in a timely manner. The OIG seeks to complete investigations within 180 days, except in unusual circumstances. This is especially critical given the

impact OIG investigations have on the lives of individuals and the activities of organizations.

- F. Complete and Accurate Documentation. The investigative report findings and investigative results (for example, indictments, convictions, and recoveries) must be supported by adequate documentation in the OIG case file. All investigative activity should be recorded in the official case file. (See IGM III-207 for instructions on establishing and organizing OIG investigative case file folders.)

200.10 Testifying in Other Than OIG Matters. Legal issues arise when OIG employees are called upon to testify in court proceedings or before administrative bodies in other than OIG matters. INV employees must notify the Deputy Assistant Inspector General for Investigations (DAIGI), through the assistant special agent in charge (ASAC) and SAC, and obtain approval before testifying or providing official OIG information in other than OIG matters. The DAIGI will obtain authorization from the OGC before any INV employee provides such information or testimony.

209.11 Use of Emergency Equipment. Agents in the INV are authorized in certain situations to use emergency lights and sirens in carrying out their official duties. Although it is impractical to frame exact guidelines that would cover all situations when the use of this equipment is warranted, some situations may include a vehicle stop for the purpose of making an arrest or executing a search warrant, a high speed pursuit (paragraph B below), or employment as a warning device (at road blocks) or when an OIG vehicle is disabled along the roadside (emergency lights only). (See IGM III-105 for further guidance.) In all cases, the paramount consideration in making use of emergency equipment will be safety.

- A. Safety. Use of emergency lights and sirens does not relieve the vehicle operator from the duty to drive with due regard for the safety of all persons using the roadways, nor does such use protect the operator from the consequences of an arbitrary exercise of the privileges granted by this policy.
- B. High Speed Pursuit Driving. High speed pursuit driving is prohibited unless the agent believes the use of emergency equipment and high speed pursuit is necessary to protect life. The capture of a fleeing felon or suspect is not, by itself, sufficient justification for high speed pursuit driving.
- C. Traffic Stops. OIG agents will not initiate vehicle stops for traffic violations.
- D. Local Law Enforcement Support. Known or anticipated situations involving arrests or felony car stops shall, if at all possible, include a briefing to the local police department and use of local police support resources. Local law enforcement support lessens any allegation of mistaken law enforcement identification and related liability issues.

- E. Approved Equipment. The DAIGI will determine the specific type of equipment to be used by the OIG. No other equipment is authorized for use.
- F. Reporting Usage.
- (1) Agents must immediately notify their supervisors after using emergency lights and siren and submit a memorandum to the DAIGI (through the SAC) within 24 hours, outlining the circumstances surrounding the use of the equipment and compliance with OIG policy.
 - (2) SACs are responsible for briefing all agents under their supervision on Inspector General policy regarding the use of emergency equipment. SACs will also review each use of emergency equipment for policy compliance and take appropriate action in cases of abuse.
 - (3) The DAIGI will review all incidents in which emergency lights and sirens were used to ensure that the usage is properly documented and in compliance with OIG policy.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 200
Ethics
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was originally issued on 5/19/97 and was re-written to reflect updates and/or changes in policies, laws, and/or guidelines.

205.1 Policy. This chapter establishes Office of the Inspector General (OIG) Investigations Division (INV) policy and procedures for receiving, processing, and determining the disposition of allegations of fraud, waste, abuse, and other misconduct. The INV shall receive and determine the disposition of complaints alleging criminal violations or administrative misconduct by Department of Justice (DOJ) employees, contractors, or grantees. The INV may elect to investigate a complaint or handle the complaint in a variety of other ways discussed in detail below.

The Inspector General may also assign certain allegations to the Oversight and Review Division for investigation.

205.2 Reference. This chapter is issued pursuant to the authority contained in the *Inspector General Act* (IG Act) of 1978 (Pub. L. No. 95-452) as amended and 28 C.F.R. §§ 27 and 0.29.

205.3 Scope. The provisions of this chapter apply to all employees of the OIG INV.

205.4 Reporting Complaints. All allegations of criminal wrongdoing or serious administrative misconduct by DOJ employees, contractors, and grantees must be reported to the OIG, except as provided in C and D below. Individuals may report allegations directly to the OIG or to a DOJ component supervisor or internal affairs office for referral to the OIG.


A. Where to Report Allegations. Complaints may be reported to INV Headquarters or to any OIG field office, area office, or domicile.

B. Information to Report. Reporting should include the identity of the complainants, subjects, witnesses, and victims and details of the allegations and corroborating evidence as soon as such information is known.

C. Coordination with the Office of Professional Responsibility – DOJ Attorney Misconduct. Allegations of misconduct by DOJ attorneys that relate to the exercise of the attorney's authority to investigate, litigate, or provide legal advice shall be reported to the DOJ Office of Professional Responsibility (OPR).

(1) Allegations of misconduct by DOJ law enforcement personnel shall be reported to DOJ OPR when such allegations are related to allegations of attorney misconduct within the jurisdiction of DOJ OPR.

(2) Allegations of unauthorized leaks of official information or abuse of position involving DOJ attorneys that are received in a field office must be reported to the special agent in charge (SAC), Operations Branch, INV Headquarters, prior to disposition. The SAC, Operations Branch, will discuss the complaint with DOJ OPR to determine whether the OIG or DOJ OPR will assume investigative jurisdiction. (b) (7)(E)



- (3) If an allegation within the jurisdiction of DOJ OPR is reported to the OIG, the SAC of the office receiving the complaint shall notify the SAC, Operations Branch, INV Headquarters, who is responsible for transmitting the complaint to OPR. If DOJ OPR receives a complaint that is within the jurisdiction of the OIG, that office should transmit it to the OIG.

- D. Federal Bureau of Investigation Whistleblower Complaints. A Federal Bureau of Investigation (FBI) employee who believes that another employee of the FBI, or of any other DOJ component, has taken or failed to take a personnel action as a reprisal for a protected disclosure may report the alleged reprisal to either the OIG or DOJ OPR.

205.5 Reporting Complaints – Classes of Complaints. Typical employee, contractor, and grantee misconduct has been categorized into three classes based on the seriousness of the offense and the effect that the offense, if proven, is likely to have on the ability of DOJ to conduct the public's business. Each of the three classes requires a different manner and level of reporting to the OIG by component managers. To establish and maintain consistency, the OIG has disseminated these offense classes and reporting requirements to DOJ managers, including components with internal affairs units (Appendix A).

- A. Classification No. 1. Allegations against an employee, contractor, or grantee that would likely result in criminal prosecution if substantiated or allegations of serious administrative misconduct against a DOJ employee of the rank of GS-15 or above. Class 1 allegations require immediate reporting to the OIG.

DOJ components and managers should not delay initial reporting to collect additional information regarding the allegation.

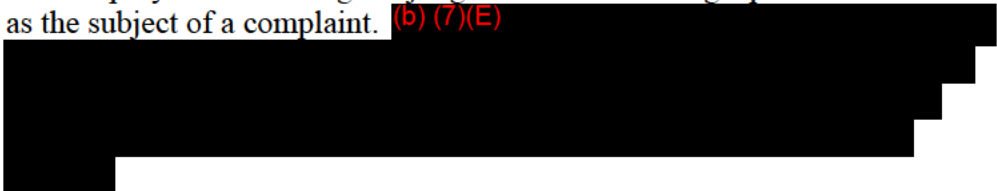
- B. Classification No. 2. Allegations against an employee, contractor, or grantee that involve violations of rules, regulations, or law that would not likely result in criminal prosecution if substantiated or allegations of serious administrative misconduct against an employee of a rank up to and including GS-14. Reporting to the OIG shall occur within 48 hours (excluding weekends and holidays).

A DOJ component that has an internal affairs-type office may begin an investigation as soon as it is aware of a class 2 allegation. However, the OIG reserves the right to initiate an investigation upon notice to the component, at which time the component must terminate its investigation.

- C. Classification No. 3. This classification consists of allegations of employee, contractor, or grantee misconduct that has minimal impact on the programs or operations of the component and is not likely to result in termination, demotion, debarment, or lengthy suspension if substantiated. Class 3 allegations will be reported monthly to the OIG in a mutually agreed upon format.

Components may initiate inquiries into class 3 allegations as soon as the components become aware of them. However, the OIG reserves the right to investigate a matter upon notice to the component, at which time the component must terminate its investigation.

205.6 Processing Complaints. All INV employees are authorized to receive complaints of misconduct. Every complaint must be recorded in the Investigations Data Management System (IDMS) as soon as it is received. IDMS will automatically assign a tracking number, called a “complaint number,” which shall be the basis for all subsequent files and records related to that complaint.

- A. Responsibility for IDMS Entry. Except as provided in (1) and (2) below, the office receiving a complaint will be responsible for entering it into IDMS.
- (1) Complaints received at INV Headquarters may be referred to the appropriate field office for input into IDMS.
 - (2) If an OIG field office receives a complaint that falls under the primary responsibility of another field office, the receiving office shall enter the complaint into IDMS and then forward the information to the responsible field office for disposition.
- B. IDMS Requirements. Specific responsibilities follow for OIG employees who receive complaints and assign them to other employees and for OIG employees who record complaints in IDMS:
- (1) OIG employees must use good judgment when entering a person into IDMS as the subject of a complaint. (b) (7)(E)

 - (2) To avoid duplication of complaints and effort, the OIG employee receiving or entering a complaint shall make reasonable queries of IDMS for existing related complaints.
 - (3) A complaint may involve more than one subject. Whenever multiple subjects are reasonably related to the same complaint, only a single complaint list with multiple subjects will be entered into IDMS.
 - (4) Multiple complainants may also make the same allegations. In such cases, a single complaint list with multiple complainants will be entered into IDMS.
 - (5) If a DOJ employee has been offered something of value (a bribe) in connection with the employee’s official duties and cooperates with the OIG,

the employee will not be listed as the subject of the complaint. The name of the non-employee person attempting to bribe the employee will be shown as the subject, with a notation that the subject is a “non-employee.”

- (6) The first allegation code entered into IDMS should describe the most serious offense. The narrative portion of the complaint must, at minimum, address the first allegation code. The narrative must be sufficient to justify the ultimate disposition of the complaint.
- (7) Civil rights or civil liberties allegations and complaints require specific IDMS entries:
 - a. Allegations of civil rights or civil liberties violations will reflect “688” as the last IDMS code for each subject. The first code will address the specific offense.
 - b. A civil rights or civil liberties complaint determined to be a *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (Patriot Act) violation will have the “Patriot Act” field checked in IDMS by INV Headquarters.
- (8) An employee receiving or entering a complaint shall ensure that the OIG manager responsible for determining the disposition of the complaint is aware that the complaint has been received.
- (9) A supervisor who receives and reviews a complaint shall ensure that all relevant information is recorded in IDMS as soon as possible after receiving the complaint.
- (10) Technical requirements for entering complaints into IDMS are contained in the IDMS Users Manual.

- C. Deleting IDMS Entries. Only INV Headquarters has the authority to delete a duplicate or erroneously entered complaint from IDMS. (b) (7)(E) [REDACTED]
[REDACTED] Requests for deletions should be made in writing to the Operations Branch or Special Operations Branch. However, field offices may modify erroneous entries of specific complaint data, such as the spelling of a name, a person’s title, date of birth, or date of incident.

205.7 Disposition of Complaints. The INV will investigate, refer, or otherwise dispose of each complaint alleging criminal or non-criminal violations by DOJ employees, contractors, or grantees.

- A. Responsibility for Disposition of Complaints. Field office SACs and INV Headquarters SACs (Operations Branch and Special Operations Branch) have

specific responsibilities for the disposition of complaints. These responsibilities vary according to the specific component from which a complaint arises. Each SAC has either a primary responsibility or a consulting responsibility for each complaint within his or her area. The following table outlines those responsibilities.

Component	Primary Responsibility	Consulting Responsibility
Bureau of Alcohol, Tobacco, Firearms, and Explosives	SAC, Special Operations	Field Office SAC
BOP	Field Office SAC*	SAC, Operations
DEA	SAC, Special Operations	Field Office SAC
FBI	SAC, Special Operations	Field Office SAC
Executive Office for U.S. Attorneys	SAC, Operations	Field Office SAC
U.S. Marshals Service	Field Office SAC*	SAC, Operations
Offices, Boards, Divisions	SAC, Operations	Field Office SAC
Patriot Act Allegations	SAC, Special Operations	Field Office SAC

* Refer to the paragraph describing monitored referrals (Inspector General Manual, Volume III, Chapter 205.8B (III-205.8B)).

- (1) The SAC with primary responsibility for the disposition of a complaint shall ensure that the disposition decision is recorded in IDMS.
- (2) Each complaint disposition generates specific requirements for additional data to be entered into IDMS. Employees should consult the IDMS Users Manual for the specific requirements of each disposition.

B. Disposition Timeframes. Each complaint should have a disposition before the end of the second business day following its receipt. Exceptions to this general rule include complaints in which a decision from the DOJ Civil Rights Division (CRT) is pending or in which other extraordinary circumstances prevail.

205.8 Disposition of Complaints – Criteria and Procedures.

A. OIG Investigations – IDMS Classification “I.”

- (1) Criteria. The following factors shall be evaluated when making a decision to classify a complaint as an OIG investigation:
 - a. The allegation constitutes a violation of federal or state criminal laws, and there is a reasonable likelihood that the matter would result in criminal prosecution by a United States Attorney or other prosecutor if proven.

This does not usually include off-duty (non-job related) misconduct prosecuted by local authorities as a misdemeanor.

- b. The allegation would likely result in a significant administrative action against a DOJ contractor, grantee, or employee at the grade of GS-15 or above if proven.
- c. The allegations are of extraordinary public interest or the subject of significant public attention.
- d. Reprisal is alleged by an FBI employee who has made a protected disclosure (FBI Whistleblower complaint). Also see Section III-205.9 below.
- e. Allegations that would normally be classified as monitored referrals, but the component has no internal investigations-type office and requests that the OIG conduct the investigation.

(2) Procedures. When a complaint is classified as an “Investigation,” it will be assigned to a case agent and its status recorded in IDMS, following the requirements outlined in the IDMS Users Manual.

(3) Dissemination. The SAC with primary responsibility for the disposition of a complaint will disseminate a copy of the complaint to the internal affairs unit of the affected component (b) (7)(E) . IDMS will create the applicable form for transmittal.

- a. (b) (7)(E)
- b. When significant additional information is received that expands the scope of a complaint, the OIG will disseminate a copy of the additional information to the component under the same circumstances as the original notification.

B. Monitored Referrals – IDMS Classification “R.” The INV may refer certain complaints as monitored referrals to DOJ components that have an Internal Affairs Office or OPR. For a monitored referral, the component conducts an investigation of the allegations and forwards a report of its completed investigation to the OIG for review. The SAC, Operations Branch, or the SAC, Special Operations Branch, INV Headquarters, will make the final determination as to which complaints are classified as monitored referrals.

- (1) Criteria. Disposition as a monitored referral is appropriate for allegations of non-criminal misconduct by an employee, contractor, or grantee. Monitored referrals may also include allegations of minor criminal misconduct that are not likely to be accepted for prosecution but will likely result in disciplinary action if proven. (Monitored referrals may also include off-duty local prosecutions that will likely result in disciplinary action if proven.) Monitored referral of a complaint can be considered when the subject employee is at the rank of GS-14 or below. In determining which complaints should be disposed of as monitored referrals, the factors to be considered include:
 - a. credibility of the complainant or other sources of information;
 - b. the ability to identify the subjects and witnesses;
 - c. seriousness of the alleged misconduct;
 - d. relationship of the alleged misconduct to the programs and operations of the component; and
 - e. potential impact that the misconduct may have on the public's view of the component's ability to carry out its mission efficiently and effectively.
 - (2) Procedures. When a complaint has been classified as a monitored referral, a record of its status must be entered into IDMS. See the IDMS Users Manual for further information. IDMS will create and save the applicable transmittal form.
 - (3) Dissemination. Monitored referrals are necessarily disseminated to the appropriate DOJ component. If information is received that expands the scope of the original complaint, a copy of the additional information will also be forwarded to the component under the same circumstances as the original referral.
- C. Management Review – IDMS Classification “M.” A complaint that does not warrant handling as an investigation or monitored referral will be forwarded to the DOJ component whenever it constitutes a matter that the component should either be aware of or act on.
- (1) Criteria. Complaints that can best be handled either by an immediate supervisor or within the chain of command should be classified for management review. Also, nonfrivolous allegations of waste, fraud, and abuse that do not involve serious individual employee misconduct should be brought to the attention of component management for review and possible corrective action under this classification.
 - (2) Procedures. The SAC with primary responsibility for determining the disposition of a complaint is responsible for forwarding it to the affected components. A component, including those with internal affairs units, may choose to conduct an

inquiry or investigation of a complaint referred for management review; however, it is under no obligation to report the results to the OIG.

- (3) Dissemination. IDMS requires that the disposition be recorded as outlined in the IDMS Users Manual. IDMS creates and stores the appropriate transmittal forms for complaints that are referred for management review.
 - (4) Complaints Not Related to DOJ. If the subjects or subject matter of a complaint is outside the jurisdiction of the OIG, the OIG employee receiving the allegations will document the complaint in IDMS (using the management review classification). Employees will not refer the reporting complainants to other agencies.
 - a. The SAC, Operations Branch, or SAC, Special Operations Branch, INV Headquarters, will refer the documented complaint to the appropriate agency.
 - b. A complaint of criminal activity not involving DOJ employees, contractors, or grantees will also be referred to the appropriate state, local, or federal law enforcement agency.
- D. Information – IDMS Classification “F.” A complaint may be classified as information and filed in the office where it was received if the complaint lacks sufficient basis or detail to warrant any follow-up by either the OIG or any DOJ component. The complaint relates to the DOJ. Copies of complaints classified “F” will not be disseminated.
- E. Consolidated – IDMS Classification “C.” An allegation may possibly be reported to the OIG more than once, either by different complainants or through different sources. Because procedures for the receipt of complaints require that IDMS be queried before a complaint is entered, instances of duplicate complaints should be rare. However, circumstances can occur where a matter that initially appeared to be independent is later determined to be related to a prior complaint. In this instance, the SAC having primary responsibility for disposition of the complaint may consolidate a complaint with one that was already recorded and classified in IDMS.
 - (1) When a complaint is disposed of as consolidated with another, that status must be recorded in IDMS, including the number of the complaint into which it is being consolidated.
 - (2) The SAC with primary responsibility will forward a copy of the consolidated complaint to the appropriate DOJ component.
- F. Non-DOJ – IDMS Classification “X.” If the correspondence has no connection with DOJ persons or programs, it will be classified using the “X” code.

- (1) Examples. The following are examples of correspondence that merit an “X” classification code:
 - a. correspondence received by the OIG that indicates a complaint falling within the investigative jurisdiction of a federal agency outside of the DOJ;
 - b. correspondence received by the OIG that indicates a complaint falling within the investigative jurisdiction of a state or local agency; and
 - c. correspondence received by the OIG that lacks adequate information to determine investigative jurisdiction.

- (2) Processing.
 - a. The Complaints Notebook in IDMS allows for only one offense code to be entered. One of the two offense codes, 498 or 598, will be used for all classification “X” complaints. Additionally, for each subject that is listed within a complaint, the same code, either 498 or 598, should be entered as the primary offense code and then a second, third, or fourth offense code can also be added if necessary.
 - b. Complaints classified as “X” require only indexing of the name of the person(s) providing the information and the name of the subject(s), if identified.
 - c. The narrative of the complaint in the Complaints Notebook Scratchpad does not have to summarize the information, as normally required but should include a one- or two-sentence indication of the nature of the information and INV disposition of the matter.
 - d. The Operations Branch will forward non-DOJ correspondence and complaints to the proper entities; however, this newly created “X” classification code will allow the field offices to also forward non-DOJ information to federal, state, or local offices as well and to track such correspondence through IDMS.
 - e. Transmittal letters are generated through a drop-down field in the Complaints Notebook and are tracked through iManage.

205.9 Processing FBI Whistleblower Complaints. When an employee of the FBI makes a qualifying complaint of reprisal (an FBI Whistleblower complaint), the complaint may be investigated by either the OIG or DOJ OPR. For every qualifying complaint received, the Senior Counsel to the Inspector General will consult with DOJ OPR to determine which office will be responsible for the investigation.

- A. Timeframes. Within 15 days of receipt of the complaint, the consultation must be completed and notification sent to the complainant as to which agency will conduct the investigation.
- B. Factors. While such factors as workload and resources should be taken into consideration in deciding which agency will conduct the investigation, the Attorney General may designate either the OIG or DOJ OPR to conduct the investigation. However, this decision is normally determined between the OIG and DOJ OPR.

205.10 Civil Rights Complaints. When a complaint alleges a violation of the federal civil rights statutes (18 U.S.C. §§ 241-242), DOJ policy requires that the Criminal Section of DOJ Civil Rights Division (CRT) review the allegation for prosecutorial merit before the OIG makes a disposition. (See the Inspector General Manual, III-224.)

- A. Timeframes. The SAC with primary responsibility for a civil rights complaint shall refer the complaint to CRT within 24 hours of initial receipt.
- B. Patriot Act Complaints. A complaint made pursuant to the Patriot Act, section 1001(Patriot Act complaint), is likely to be, but not necessarily required to be, handled as a civil rights complaint. This will depend on the specific nature of the allegations.
- C. Complaints Pending CRT Decision. While a complaint is pending an initial prosecutorial decision from CRT, its disposition in IDMS will remain unclassified. However, information must be entered into IDMS detailing the referral to CRT (classification code "U"). (See the IDMS Users Manual.) The OIG shall send notice of the CRT referral to the component where the subject is employed (IDMS provides the applicable form). If CRT does not notify the OIG referring office of its prosecutorial opinion in a timely manner, that office shall follow up in order to determine CRT's decision.
- D. Disposition. When the OIG receives CRT's decision, the responsible SAC must record the decision in IDMS, including any changes in the status of the complaint.
 - (1) CRT may accept the complaint and assign it to the OIG for investigation. If so, follow the procedures outlined in Section III-205.8A, above.
 - (2) If CRT declines prosecution, the SAC with primary responsibility may open an administrative investigation, make the matter a monitored referral, or forward the complaint to the appropriate component for management review.
 - (3) If CRT assigns a criminal investigation to the FBI, the OIG may open an administrative investigation but only after consultation with the FBI.
- E. Preliminary Inquiry. The OIG may receive a complaint alleging a civil rights violation that lacks sufficient specificity to refer to CRT for its opinion. When this

occurs, the SAC with primary responsibility may obtain additional predicated material before submitting the complaint to CRT for its opinion. Such a preliminary investigation (classification code "U") must never exceed 60 days. In determining whether to conduct such a preliminary investigation, the SAC should consider the likelihood that further predicated material will be available and the resources necessary to obtain such material.

- 205.11 Confidentiality of Complainants and Witnesses. The IG Act places a duty upon the OIG to protect the identity of a federal employee who files a complaint unless disclosure of the employee's identity is deemed unavoidable in the conduct of an investigation. The OIG also has a strong interest in maintaining the confidentiality of other individuals who cooperate with the OIG on the condition that their identities are protected.
- A. Disclosure Considerations. In conducting and supervising investigations, OIG employees must weigh the interest in maintaining employee confidentiality and the right to be protected from retaliation against the need to provide the component with all of the information necessary to take administrative action.
- B. Confidentiality Policy. When a component is to be provided a copy of any complaint, all OIG employees must adhere to the following policy:
- (1) Complainants. When a complaint is disseminated, complainants will not be identified, either by name or by other means, unless at least one of the following conditions exists:
- a. The complainant is not a federal government employee, contractor, subcontractor, grantee, sub-grantee, or person with an ongoing relationship with the federal government. The complainant's relationship should be ascertained by a search of IDMS and a reading of the complaint material.
 - b. Component management provided the complainant's identity to the OIG with the complaint.
 - c. At the time of the complaint or when subsequently contacted, the complainant affirmatively agrees that his or her identity may be revealed to the component. (See paragraph D(1) below.)
 - d. Based on information contained in the complaint, or otherwise known to the OIG, there is a reasonable basis for the OIG to view the complainant as posing a potential threat to the safety of himself/herself or others, and there is a reasonable basis for the OIG to believe that revealing the complainant's identity would be a reasonable step to mitigate the potential threat. Prior to revealing the complainant's identity to a component or other appropriate entity, approval must be provided by the Assistant Inspector General for Investigations or his or

her designee, except that the complainant's identity may be revealed without such approval when exigent circumstances, such as an imminent threat of violence, require immediate action. The Inspector General has determined that revealing the complainant's identity under these circumstances would be deemed unavoidable in the conduct of an investigation, and therefore permitted under the IG Act.

- e. The complainant is a federal employee of a non-DOJ component. In this case the complaint should be forwarded to the OIG for the complainant's organization and the complainant notified that the complaint was forwarded.
- f. Any other matter as determined by the Inspector General.

(2) Witnesses. When a complaint is disseminated, witnesses are usually identified unless one of the following conditions exists:

- a. The witness provided information to the OIG on the condition that his or her identity would be kept confidential.
- b. The witness expressed fear of reprisal if his or her identity was disclosed.

(3) Question Regarding Circumstances. If there is any question whether one of these conditions applies to the circumstances, then the complainant or witness should not be identified.

C. Retaliation Prohibitions.

- (1) It is a violation of the IG Act for a supervisor to retaliate against an employee who has provided information to the OIG. Any individual responsible for retaliation against an employee who engaged in a protected activity (including providing information regarding an internal investigation) may be disciplined by the head of the component agency.
- (2) At the time a complaint or report of investigation is disseminated to a component, the INV will advise the component that complainants and witnesses who are identified in the report are entitled to protection from retaliation under the IG Act and the *Whistleblower Protection Act*. This advisory is printed on the field office form used to disseminate complaints to components (Appendix B).

D. Disclosure Requests. If in order to address a matter appropriately, the employing component requests that the OIG identify a complainant or witness whose identity has been kept confidential, the OIG will seek permission from the complainant or witness to disclose the information.

- (1) If the complainant or witness agrees that his or her identity may be disclosed, the complainant will sign a “reveal letter” so stating. (See Appendix C for a sample letter.)
- (2) If the complainant or witness does not give permission, identifying information will not be disclosed unless the Assistant Inspector General for Investigations determines that the need for disclosure outweighs the individual’s interest in confidentiality. The individual so affected will be advised that his or her name will be provided to the component.

205.12 Processing Allegations of Sexual Abuse in Confinement Settings.

- A. Disposition. 28 C.F.R. § 115.71 mandates that all allegations of sexual abuse or sexual harassment of inmates by staff members, contractors, or volunteers will be investigated promptly, thoroughly, and objectively, including allegations received from third parties and anonymous reports. If initial review or preliminary investigation of the allegation determines that it is unlikely to result in a criminal prosecution, the SAC or ASAC of the field office of jurisdiction may request that the allegation be referred to the component for investigation. The referral will be made by the relevant INV Headquarters Operations Branch, in consultation with the field office. All such referrals will be monitored referrals unless no additional investigative steps are necessary or if the conduct, as reported and if true, would not amount to a serious administrative violation, in which case a management referral may be considered. See also Appendix D for definitions of sexual abuse and harassment terms in the *Prison Rape Elimination Act (PREA)*.
- B. IDMS and iManage.
 - (1) The field office will upload predicated documents to iManage prior to requesting an investigative disposition from INV Headquarters.
 - (2) Complaint code 603 will be used for allegations of sexual abuse of inmates and detainees, including inappropriate relationship allegations with an implied likelihood of sexual abuse. In such cases, the PREA box on the IDMS complaint form should be checked.
 - (3) Complaint codes 603, 605, or 610 will be used for allegations of sexual harassment of inmates and detainees, depending on the nature of the harassment, and the PREA box on the IDMS complaint form should be checked. In such cases, complaint code 703 will not be used, as it applies only to sexual harassment as a personnel issue.
 - (4) Allegations that do not fit the PREA definition of sexual abuse or harassment, such as allegations involving pat-down searches that appear to be within the scope of official duties, within current DOJ policy, and not for the purpose of sexual abuse or gratification, can be coded with any appropriate offense code,

including 412. It is not necessary to check the PREA box on the IDMS complaint form, regardless of whether the complainant subjectively characterized the actions as “sexual abuse.”

- C. Inmate-on-Inmate Sexual Abuse. All allegations of sexual abuse or sexual harassment of inmates by other inmates will be referred immediately to the component.
- (1) BOP.
- a. Inmate-on-inmate allegations will be referred immediately by the office of receipt to the BOP’s PREA Coordinator Hotline, [REDACTED] (b) (7)(E) [REDACTED] for subsequent referral to the relevant BOP institution and to the FBI. It is not necessary to enter the complaint in IDMS prior to referring the predication to the BOP’s PREA Coordinator, but entry of the complaint in IDMS will be done as soon as possible after referral. Use the appropriate complaint code (that is, 603, 605, or 610); check the PREA box in IDMS; and assign a disposition of “X.” Do not refer the allegation to the BOP’s Office of Internal Affairs.
- b. If the complaint involves both inmate-on-inmate allegations and staff misconduct or negligence, including staff enablement of inmate-on-inmate sexual abuse through willful or gross negligence, it will be treated as an employee misconduct allegation. All correspondence with the BOP concerning the allegation will be directed to the BOP’s Office of Internal Affairs. Such allegation will not be referred to the BOP’s PREA Coordinator.
- (2) USMS.
- a. Inmate-on-inmate allegations will be classified in IDMS as an “X” and referred to the USMS’s Office of Internal Investigations. Use the appropriate complaint code (that is, 603, 605, or 610) and check the PREA box in IDMS.
- b. If the complaint involves both inmate-on-inmate allegations and staff misconduct or negligence, it will be treated as an employee misconduct allegation.
- D. Confidentiality. If an inmate affirmatively requests confidentiality in connection with an allegation of sexual abuse or sexual harassment that he or she reports directly to the OIG, that request will be honored. If it is determined that disclosure of the inmate’s identity to the component is necessary for investigative reasons or in connection with a referral of the complaint, the field office will contact the inmate either in person or via mail and request that the inmate sign a release of identity form.

If the inmate refuses, a referral of the complaint to the component will only be made after the inmate's identity is redacted from the complaint form and predicated materials.

- E. Acknowledgment Letters. It is not necessary to send an acknowledgment letter to inmates who report violations via e-mail to the PREA Hotline. The Hotline was established to afford inmates a method of reporting sexual abuse violations without the BOP having a record of their complaint. The e-mails are not captured at the institution, and no local record exists of inmate e-mail communication with our offices. The "reply" function is disabled; we are not able to send the inmates a direct e-mail response to their complaints, which would create a record that would defeat the security protocol. Inmates are informed by the BOP that they will not receive a response to e-mails to our offices. Sending a written acknowledgment letter is not advised unless the inmate specifically requests one because an envelope with an OIG return address could alert institution staff that the inmate very likely filed a complaint.

APPENDIX A

Typical Types of Misconduct To Be Reported to the OIG

(This list is not meant to be all inclusive)

TYPICAL TYPES OF MISCONDUCT TO BE REPORTED TO THE OIG

(This list is not meant to be all inclusive)

Classification No. 1

(Immediate Reporting)

- Bribery, graft, or conflict of interest, including an offer or acceptance of anything of value
- Extortion
- Fraud
- Theft, conversion, or embezzlement of funds or property in an amount greater than \$100
- Sale, possession, or trafficking in illegal drugs
- Submission of false claims
- Perjury or false statements
- Concealment, removal, or mutilation of official documents
- Conflict of interest
- Smuggling or trafficking in contraband
- Providing contraband to any person in custody
- Sexual contact between employees and persons in custody, aliens, informants, protected persons, undercover operatives, persons under investigation, or persons seeking benefits from the DOJ
- Discrimination or sexual harassment accompanied by violence, physical force, or other egregious misconduct
- Use of a firearm in a manner that appears to constitute a violation of law or DOJ regulations
- Criminal civil rights violations
- Assault
- Facilitating the escape of any person in custody
- Unauthorized disclosure of sensitive information, including information in any electronic system
- Unauthorized interception of wire or oral conversations
- Class 1 misconduct attempt, conspiracy, obstruction of justice, aiding and abetting, or concealment or failure to report any matter in class 1

Classification No. 2

(48-Hour Reporting)

- Assault, threatening assault
- Use of Government facilities, supplies, equipment, services, personnel, or identification for other than official purposes
- Off duty misconduct resulting in a felony arrest or conviction

- Discrimination and sexual harassment not included in class 1
- Outrageous or unprofessional conduct
- Breaching the safety or security of a DOJ program or operation, resulting in escape or serious injury, disclosure of confidential informants or other protected persons, or endangerment of employees, contractors, and clients of the DOJ
- Use of a government credit card for other than its intended purpose in an amount greater than \$1,000
- Gambling or promotion of gambling on government property
- Destruction of government property
- Inappropriate relationships between employees and persons in custody, aliens, informants, protected persons, undercover operatives, persons under investigation, or persons seeking benefits from the DOJ, not included in class 1
- Unauthorized release of information not included in class 1
- Failure to properly account for funds, valuables, and personal property of persons in custody
- Falsification of employment documents
- Attempt, conspiracy, obstruction, aiding and abetting, concealment, or failure to report any matter in class 2

Classification No. 3

(Monthly Reporting)

- Disorderly conduct or abusive language
- Prohibited personnel practices not included in class 1 or 2
- Conducting personal business during duty hours
- Refusal or failure to follow instructions or procedures, failure to respond to an emergency, failure to properly supervise or control persons in custody
- Off-duty misconduct resulting in misdemeanor arrest
- Unauthorized use/misuse of a government vehicle
- Failure to honor just debts
- Accidental discharge of a firearm that does not result in injury to anyone
- Use of a government credit card for other than its intended purpose in an amount not exceeding \$1,000
- Violations of security regulations
- Intoxication or consumption of alcohol while on duty

APPENDIX B

**Field Office Form for Dissemination/Referral of
Complaints to DOJ Components**

(Date)

MEMORANDUM FOR _____, Chief Inspector
Office of Internal Affairs
U.S. Marshals Service

FROM: Special Agent In Charge
_____ Field Office

SUBJECT: OIG Complaint No. _____
Agency File No. _____
Subject _____

This matter is referred for appropriate disposition by Agency management in accordance with your Agency's policies and regulations. A copy of your findings or final action is not required by the OIG.

This matter is referred to your Agency for investigation. Please report the status of this matter in your monthly report to the OIG. A copy of your findings or final action is required to be provided to this field office.

This complaint will be investigated by the OIG.

OIG disposition awaits the prosecutorial decision of the Civil Rights Division.

IMPORTANT NOTICE

Identifying information may have been redacted from the attached OIG Complaint Referral in accordance with the *Inspector General Act*, Section 7, or because an individual has: (a) requested confidentiality or (b) expressed a fear of reprisal. If you believe that it is necessary that redacted information be made available to your Agency, you may contact the Assistant Inspector General for Investigations.

Please be advised that where adverse action is not contemplated, the subject of an investigation does not have a right to have access to an OIG Complaint Referral or to the identities of complainants or witnesses and that in all cases, complainants and witnesses are entitled to protection from reprisal pursuant to the *Inspector General Act* and the *Whistleblower Protection Act*.

Special Agent in Charge

Date

Attachment

APPENDIX C

Sample Reveal Letter

(DOJ Letterhead)

(Date)

(Full Name and Address)

Dear (Name):

The Office of the Inspector General (OIG) has received your correspondence and reviewed the information you provided. After careful consideration and in view of the limited resources of the OIG, we have decided not to open an investigation of the allegations you raise.

However, we believe that the issues you raise should be brought to the attention of the responsible component/agency for possible administrative inquiry and management review. We would therefore like to forward your correspondence to the _____ for further action.

Please indicate by marking the appropriate box below whether and under what conditions you consent to the OIG forwarding your complaint to this component/agency. Return this consent decision to us in the enclosed, pre-addressed envelope. A copy is included for your records.

Your response is appreciated and time sensitive. If you do not return your consent decision to us within two months of our mailing date, the OIG will close the matter and take no further action regarding your complaint.

If you have any questions, please contact us again.

Sincerely,

(Signature Block)

- I understand and agree that the OIG will forward my complaint to the component/agency designated above and that my identity will be revealed to that component/agency.
- I understand and agree that the OIG will forward my complaint to the component/agency designated above with my identifying information redacted. I further understand that this may limit the ability of this component/agency to investigate or review my complaint.
- I do not consent to the OIG forwarding my complaint for further action. I understand that this will preclude any review of my complaint.

Signature

Date

APPENDIX D

Definitions of Terms in the *Prison Rape Elimination Act*

DEFINITIONS OF TERMS IN THE *PRISON RAPE ELIMINATION ACT*

The definition of *sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer* includes any of the following acts, with or without consent of the inmate, detainee, or resident:

- (1) contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) contact between the mouth and the penis, vulva, or anus;
- (3) contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (4) penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (5) any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (6) any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1)-(5);
- (7) any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of an inmate, detainee, or resident, and
- (8) voyeurism by a staff member, contractor, or volunteer.

Voyeurism by a staff member, contractor, or volunteer means an invasion of privacy of an inmate, detainee, or resident by staff for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring an inmate to expose his or her buttocks, genitals, or breasts; or taking images of all or part of an inmate's naked body or of an inmate performing bodily functions.

Sexual harassment in a confinement setting includes:

- (1) repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- (2) repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 205
Handling Complaints
Revisions

This chapter was previously revised on April 22, 2009, April 23, 2007, and originally issued on September 22, 1997. This chapter has been rewritten to reflect updates and/or changes in policies, laws, and guidelines.

This chapter includes an inserted revised policy approved by the Inspector General or his Designee, issued December 1, 2014:

Changes, additions, and deletions in guidance issued December 1, 2014, appear in the following sections:

- 205.11:** Changes guidance in the last sentence of the unnumbered first paragraph, replacing “identities are kept secret” with “identities are protected.”
- 205.11B(1):** Adds guidance that precludes complainant identification by other means in addition to precluding complainant identification by name.
- 205.11B(1)a, d, e, and f:** Add identity protection exception conditions.

This chapter revision includes an inserted revised policy, approved by the Inspector General or his Designee, issued July 9, 2014:

This policy addition is in conformance with the Prison Rape Elimination Act (PREA), Public Law 108-79, which was passed unanimously by Congress in 2003, and AG Order No. RIN 1105-AB34, as codified in the Code of Federal Regulations (C.F.R.), Title 28, Part 115, on May 16, 2012. (See also www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf.)

- 205.12:** Adds guidance concerning processing and investigation of allegations of sexual abuse in confinement settings (Policy Memorandum FY 14-POL-03).

Appendix D: Adds Definitions of Terms in the *Prison Rape Elimination Act* (Policy Memorandum FY 14-POL-03).

Changes, additions, and deletions in guidance issued April 22, 2009, appear in the following sections:

- 205.4:** Corrects paragraph reference in the first sentence.
- 205.6:** Changes the database management system name to Investigations Data Management System and introduces the new acronym.
- 205.6A:** Changes guidance regarding entering complaints in IDMS, specifying exceptions.

- 205.6B(7):** Changes code and field check guidance for allegations of civil rights or civil liberties violations.
- 205.8A(3)a:** Deletes guidance requiring quarterly review (b) (7)(E) [REDACTED].
- 205.8B:** Changes guidance regarding monitored referrals, specifying components that may receive INV-monitored referrals. Changes guidance regarding off-duty local prosecutions, removing misdemeanor limitation.
- 205.8C:** Clarifies guidance regarding management review forwarding.
- 205.8D:** Clarifies guidance regarding information-level complaints.
- 205.8F:** Adds a new consolidated classification “X” and guidance for correspondence that has no connection with DOJ persons or programs.
- 205.10C:** Adds use of classification “U” for IDMS information detailing referral to CRT.
- 205.10E:** Adds use of classification “U” in IDMS for CRT preliminary investigations. Changes determination guidance in last sentence from “whether to open” to “whether to conduct.”
- 205.11D(2):** Changes guidance regarding disclosure determination time period.
- Appendix A.** Format revised.
- Appendix B.** Changes “Report/Referral” to “Complaint Referral.”
- Appendix C.** Replaces reveal letter.

- 207.1 Policy. This chapter establishes the policies, procedures, and standards by which the Office of the Inspector General (OIG) will conduct and manage investigations.
- 207.2 Reference. This chapter is issued under the Inspector General Act of 1978 (Public Law (Pub. L.) 95-452, October 12, 1978; 5 U.S.C. App.), as amended, and Attorney General Order 2492-2001. Rehabilitation Act of 1973.
- 207.3 Scope. The provisions of this chapter apply to all employees of the OIG Investigations Division (INV).
- 207.4 Opening Investigations.
- A. Geographic Areas. The field office responsible for the geographic area where the majority of relevant witnesses or evidence are located will generally open and conduct the investigation. This is generally where the predicated incident or event occurred. If there is sufficient reason for a different field office (including the OIG Fraud Detection Office) to conduct the investigation, the Special Agent in Charge (SAC), Operations Branch I or Operations Branch II, INV Headquarters, will coordinate with the field office SACs involved.
 - B. Headquarters Coordination Responsibility. The SAC, Operations Branch II, INV Headquarters, is responsible for coordinating all OIG investigations involving the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) subjects or programs. The SAC, Operations Branch I, INV Headquarters, is responsible for coordinating OIG investigations involving all other Department of Justice (DOJ) component agencies, offices, boards, and divisions.
 - C. Investigations Data Management System. The online Investigations Data Management System (IDMS) performs data compilation and case tracking functions. When a SAC or higher official decides that a complaint should be investigated, the complaint will be given a disposition of “I” (Investigation) in IDMS. (See the Inspector General Manual (IGM), Volume III, Chapter 205, “Handling Complaints” (III-205), for case opening criteria.)
 - (1) All investigations will be recorded (opened) in IDMS using one of three opening status codes: “OPCR,” criminal case; “OPAD,” administrative case (non-criminal); or “OPIN,” open initiative.
 - (2) Special Agents (SAs) and Assistant Special Agents in Charge (ASACs) will ensure that completion of all applicable fields in IDMS is consistent with policy and contemporaneous with the development of the information. Refer to the IDMS Users’ Manual for detailed information.

- D. FBI Notification Letters. Field Office SACs are responsible for notifying in writing the FBI field office with concurrent jurisdiction upon the opening of any criminal investigation for which the subject is an employee of the DOJ, a contractor, grantee, or other person or entity doing business with or receiving benefits from the DOJ. The written notification is to be made within 30 calendar days of case opening. A copy of the written notification will be uploaded into iManage. Due to the OIG's oversight role of the FBI, this notification requirement is not applicable for investigations into FBI personnel and program areas. Any notification concerning these excepted FBI investigations will be performed by INV Headquarters.

207.5 Managing Investigations.

A. General Principles.

- (1) SACs and ASACs will ensure that agents within their field offices adhere to the investigative policies, standards, and procedures established for INV. They will manage the investigative resources available within the field offices efficiently and effectively. SACs and ASACs will ensure that agents report all relevant information accurately, concisely, clearly, in a timely manner, and in the prescribed format.
- (2) Unless otherwise directed by INV managers, agents must fully and completely investigate every case to resolve all criminal aspects of the complaint. Agents also will address all administrative aspects of an investigation unless otherwise directed by INV managers or unless the conditions specified in paragraph 207.19B concerning "60 Day Cases" are met.
- (3) SACs will act as the approving authority for all investigative reports prepared by their offices.
- (4) To facilitate quick and accurate reviews by INV field and Headquarters managers, agents must regularly update their cases in IDMS. When updating the IDMS Case Status Screen (scratchpad), agents should include only concise case related information that advances the investigation.
 - a. Content. The Case Status Screen should contain only the following types of information:
 - Completed investigative activities with a brief synopsis of the outcome.
 - Case related activities/information.
 - Case accomplishments (criminal/civil/administrative).
 - b. Format. Each Case Status Screen entry will contain the following:

- The date associated with the investigative activity.
- A brief description (a few sentences) of the results of the activity.
- Once an entry is made it should not be changed or deleted.

c. Examples. Below are examples of appropriate Case Status Screen entries:

- 01/02/18 - Contracting Officer Edward Jones was interviewed. Jones provided a copy of the DEA contract file with XYZ Company.
- 01/03/18 - Robert Smith, Personnel Director for XYZ Company, was interviewed concerning the relationship between Subject Fred Brown and XYZ Company. Smith confirmed that Subject Brown was engaged in employment negotiations with XYZ Company at the time Brown awarded the contract to XYZ Company.
- 01/04/18 - Subject Fred Brown was interviewed. Brown admitted that he awarded the DEA contract to XYZ Company in order to curry favor with the company during his employment negotiations.

B. Timeframes for Working and Completing Investigations.

- (1) All investigations will be completed within 180 days or as designated by INV Headquarters. Cases with more complex and extenuating circumstances may reasonably take longer, but will be worked expeditiously. Agents should consult with a federal prosecutor at an early stage of each criminal investigation. Once the criminal aspects of a case have been completed and the remaining investigation is administrative, the case should be completed within 120 days.
- (2) The SAC/ASAC will ensure that every case is promptly and efficiently investigated, with no more than 30 days between investigative activities, and ensure that the activity is promptly and properly reported by an OIG Form III-210/4 (Memorandum of Investigation) (MOI) (*SharePoint Forms: IG Manual*).
- (3) Agents and supervisors should not record explanations for lack of investigative activity in the case file. For example, lack of investigative activity should not be recorded in the IDMS Case Status Screen or on an MOI.

- (4) The SAC may suspend the 30-day rule after completion of all investigative activity and the formal presentation of the case to a U.S. Attorney or other prosecutor for a prosecutorial decision. Once a case has been formally presented, change the IDMS case status code to “OPJP” (Open in Judicial Proceedings) and prepare an MOI reporting the status of the judicial action at least every 120 days. Discussions regarding the potential for criminal prosecution that are common between agents and prosecutors during the early stages of an investigation do not constitute a formal presentation for prosecution.
- C. Investigative Work Plans. Although not required for every investigation, the SAC/ASAC may require an OIG Form III-207/7 (Investigative Work Plan) (*SharePoint Forms: IG Manual*) if he or she considers it beneficial to the management of any investigation. The Investigative Work Plan differs from the Investigative Work Agreement for Priority Investigations that is required for all priority cases (see paragraph 207.11B below).
- (1) The case agent will normally prepare the Investigative Work Plan in conjunction with his or her supervisor. The SAC must review, approve, and sign the plan.
 - (2) The Investigative Work Plan must address the following items:
 - a. Target Completion Date. The target completion date must be no more than 180 days from the date the investigation is opened. In criminal cases, agents should have completed all investigative steps and formally presented the case to a prosecutor within 180 days.
 - b. Summary of Allegations. Include a brief summary of the predication for the investigation and the specific allegations to be addressed by the investigation.

(b) (7)(E)



(b) (7)(E)



(3) Once approved, the work plan need not be updated as the investigation progresses.

D. Operational Plans. Agents will prepare written operational plans on OIG Form III-207/10 (Operational Plan) (*SharePoint Forms: IG Manual*) when engaging in investigative activities that involve such things as executing search warrants, conducting undercover activities, complex surveillance, or multiagency operations.

(1) The purpose of thoroughly planning such activities and preparing an operational plan is to assure that the operation will be carried out in an effective, efficient, and safe manner.

(2) When planning an operation, agents will address all the applicable items listed in the sample operational plan.

E. Compliance with the Rehabilitation Act. It is the policy of the OIG not to discriminate based on disability when engaging in law enforcement programs and activities, and to afford qualified persons with disabilities equal opportunity to safely and fully participate in and benefit from such programs and activities. Agents shall be informed of and comply with the nondiscrimination and equal opportunity requirements of the Rehabilitation Act of 1973. Section 504 of the Act provides that "[n]o otherwise qualified individual with a disability in the United States * * * shall, solely by reason of her or his disability, be excluded from the participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance or under any program or activity conducted by any Executive agency." All agents will conduct investigations in compliance with Rehabilitation Act principles and with all related OIG policies and guidance issued.

207.6 Management Tools and Responsibilities.

A. Field Office Productivity Chart. The Field Office Productivity Chart, available at the INV Cyclical Report location in SharePoint, is a monthly report of IDMS data

compiled on each field office and area office and may include, among others, the following categories: ceiling, complaints, cases opened, cases closed, OPJP, OPCR/OPAD, open 6-12 months, open 12+ months, case timeliness percentage, case diversity (percentage BOP), grant fraud opened, grant fraud closed, cases with audit opened, cases with audit closed, recoveries, arrests, trials, and administrative actions.

- B. Quality, Objectivity, Timeliness, and Appropriate Direction of Investigations. The ASAC, SAC, and INV Headquarters assure the quality, objectivity, and timeliness of investigations and assure that investigative efforts are appropriately directed toward addressing the issues raised by the allegations.
- (1) ASAC. The ASAC will stay current on the status of all investigations being worked by agents under his or her supervision. The ASAC may accomplish this task through reviews of investigative work plans and operational plans, case file reviews, reviews of IDMS data, and personal discussions with the case agent. The ASAC will conduct case reviews at least every 60 days and he or she will record the date of the case reviews in each reviewed case's IDMS case status screen "scratchpad" along with his or her initials.
 - (2) SAC. The SAC will also stay current on the status of investigations through in-person discussions with the ASAC and case agent and reviews of work plans, operational plans, and case files, as well as reviews of IDMS data. The SAC is ultimately responsible for the quality, objectivity, timeliness, and appropriate direction of all investigations being conducted by his or her field office.
 - (3) INV Headquarters. INV Headquarters management personnel shall review priority investigations and over-age investigations, primarily through quarterly video teleconferences with field office supervisors; reviews of various reports, such as the Field Office Productivity Chart and reviews of IDMS data.

207.7 Office Case File Folder. A case file folder will be established immediately upon opening and assigning an investigation. All information and original documents pertaining to the investigation will be maintained in an office case file folder bearing the appropriate case number. All documents placed in the case file folder must be uploaded to iManage contemporaneously with their addition to the case file. A book-type folder, brown, hard cover, with six divisions, will be used to house office case files until INV implements an official electronic case file system. The office case file folder is the property of the OIG and may not be removed from the office.

- A. Work Folders. A case agent may create a working case folder into which he or she may place copies of documents entered in the office case file folder. The working case file is also the property of the OIG, but as it contains only duplicates of

material in the office case file, it may be removed from the office during the investigation, as needed. All OIG employees must take care with working case files to safeguard their contents from loss or unauthorized disclosure.

B. Document Placement in the Office Case File Folder.

- (1) Information and documents received or created during the investigation (such as MOIs, sworn statements, and telephone toll records) will be maintained on the right side of the case file folder, generally in chronological order.
- (2) The following items will be affixed to the inside of the left cover of the case file folder:
 - a. an up-to-date copy of the IDMS complaint/case form;
 - b. OIG Form III-207/1 (File Content Summary Sheet) (*SharePoint Forms: IG Manual*);
 - c. OIG Form III-207/7 (Investigative Work Plan) (*SharePoint Forms: IG Manual*), if applicable;
 - d. OIG Form III-207/6 (Case Review Record) (*SharePoint Forms: IG Manual*); and
 - e. OIG Form-207/8 (Investigative Work Agreement for Priority Investigations) (*SharePoint Forms: IG Manual*), if applicable.

C. File Content Summary Sheet and Case Review Record.

- (1) The case agent will record on the File Content Summary Sheet, by date of entry and description, all documents, including MOIs, placed in the case file and all evidence turned over to the evidence custodian.
- (2) As needed, the ASAC or SAC will review the contents of the file to ensure that all investigative matters are completed in a timely manner and ensure that the case file meets all administrative requirements. Formal case reviews are to be conducted at least every 60 days. The SAC or ASAC may use the Case Review Record (*SharePoint Forms: IG Manual*) and the Case Review – Supervisor’s Checklist (*SharePoint Forms: IG Manual*) to assist in reviewing the case file.

D. Special Contents. Whenever information contained in an investigative office case file relates to the following special contents items, the outside of the case folder must be conspicuously marked indicating the presence of such information:

- (1) classified documents (a case file containing classified documents also requires special storage and accountability (see IGM I-220).
- (2) identification of juveniles.
- (3) grand jury information (applies only when information is received from the grand jury and requires special storage and accountability (see IGM III-231).
- (4) (b) (7)(E) [REDACTED]
- (5) IRS income tax information (requires special storage and accountability) (see IGM III-231).
- (6) (b) (7)(E) [REDACTED]
- (7) medical information identifiable to an individual (see IGM III-231).
- (8) (b) (7)(E) [REDACTED]
- (9) compelled statements.

E. Disposition of Investigative Notes and Work Papers.

- (1) Interview notes and work papers produced during an investigation will clearly and legibly identify the source of the information, person interviewed, date of inquiry or interview, others present during the inquiry/interview, and the agent taking the notes.
- (2) When the investigation is closed, scan and then upload as a single document all agent notes to iManage with the file name "Agents' Notes" and the case number (i.e., Agents' Notes 2018-001234." Place all original notes in an envelope and attach the envelope inside the office case file folder. The envelope will be labeled "Agents' Notes." Write the full case number on the envelope.

207.8 Memorandum of Investigation. The Memorandum of Investigation (MOI) (OIG Form III-210/4) is the investigating agent's report of a particular facet of the investigation process. It will be a concise but comprehensive report of investigative activity, not just a compilation of the agent's investigative notes. See IGM III-210 and the *MOI Format and Style Standards Guide* (OIG Guide III-210/4) available on SharePoint for additional guidance.

- 207.9 Report of Investigation. To report the results of an OIG investigation, the SA will prepare a Report of Investigation (ROI) (OIG Form III-210/1), or an Abbreviated Report of Investigation (AROI) (OIG Form III-210/2), as appropriate. The ROI is the OIG’s official record of an investigation and will contain all relevant material pertaining to the investigation. When appropriate, a copy of the ROI will be provided to a prosecutor or an official in the affected DOJ component. See IGM III-210 and the *ROI Format and Style Standards Guide* (OIG Guide III-210/1) available on SharePoint for additional guidance.
- A. Review and Approval. The SAC will review each completed ROI to ensure that the ROI accurately reflects the OIG’s investigative findings and that the report is complete, concise, objective, well written, and supported by and consistent with what is recorded in the MOIs. Since the SAC is responsible for the quality of all ROIs produced by his or her field office, the SAC will ensure that the investigation meets OIG investigative standards (IGM III-200) and that the ROI conforms to the *ROI Format and Style Standards Guide* (OIG Guide III-210/1).
- B. Distribution. ROIs normally include investigations closed with a status code of “Closed – Criminal” or “Closed – Administrative.” The distribution of final ROIs (including exhibits) for closed investigations follows.
- (1) Retain the original ROI in the field office case file and upload the final ROI into iManage according to directions provided by SAC Investigative Support Branch.
 - (2) If the subject is a congressional official or political appointee, a second copy of the ROI should be submitted to INV Headquarters for distribution to the Deputy Attorney General’s Office.
 - (3) Headquarters management will consult with the Front Office to determine whether the ROI or an investigative summary will be posted to the OIG public website.
- C. Distribution Exceptions.
- (1) Federal regulations place certain limits on the distribution of reports that address retaliation allegations made by federal employees. Accordingly, the distribution of any OIG report that addresses such claims will be coordinated through the appropriate SAC, Operations Branch I or Operations Branch II, INV Headquarters. In addition, when closing a completed criminal case, the field office SAC may request that INV Headquarters not submit a copy of the final ROI to the component if all of the following conditions are met.
 - a. The allegation is not substantiated.

- b. The report contains sensitive information supplied by another agency or a confidential informant.
 - c. The SAC has determined that circumstances may warrant reopening the investigation at a later date and that the release of a report at this time may jeopardize those future efforts.
- (2) In these circumstances, the SAC must inform the SAC, Operations Branch I, or SAC, Operations Branch II, INV Headquarters, why a component copy is not being submitted to INV Headquarters. In lieu of a copy of the closing ROI, INV Headquarters will submit a memorandum to the component agency as notice of the case closure.
 - (3) For distribution of closing ROIs containing (b) (7)(E) material, see IGM III-223.

207.10 Abbreviated Report of Investigation. The Abbreviated Report of Investigation (AROI) (OIG Form III-210/2) is an optional alternative writing format for use when an investigation is being closed and can be reported in a brief synopsis. The AROI is not a chronological accounting of the investigation but, instead, must summarize the allegations and investigative findings in a few brief paragraphs. Agents must prepare AROIs in conformance with the current *AROI Format and Style Standards Guide* (OIG Guide III-210/2) issued by headquarters and posted in SharePoint.

- A. Authorization for Use. An AROI is authorized in the following circumstances.
 - (1) Cases Elapsed Not More Than 60 Days. The time period between the date the OIG received the complaint and the date the investigation is closed is not more than 60 days.
 - a. All Components. All criminal allegations have been resolved, or because the allegations lack merit, the investigation is being closed as “Information to File.”
 - b. Bureau of Prisons or U.S. Marshals Service. Bureau of Prisons (BOP) or U.S. Marshals Service (USMS) unresolved administrative issues are being forwarded as a monitored referral or for management review.
 - (2) Cases Without Regard to Time Elapsed. Regardless of the time elapsed after the complaint was received, circumstances are such that a detailed ROI would serve no useful purpose to the component, as in the following examples:

- a. Both criminal and administrative proceedings have been completed, and the findings are not going to require action by a component or program office — for example, a case where no DOJ employee was involved or was identified;
- b. The investigation did not substantiate the allegation, and the results are being reported to a program office or component; or
- c. The information being reported is a follow-up to an interim report, such as to report final judicial action. (The interim ROI will be made an exhibit to the closing AROI.)

B. Distribution.

The distribution of AROIs (including exhibits) for OIG investigations will be as follows:

- (1) Investigations Closed With a Status of Closed – Criminal (CLCR) or Closed – Administrative (CLAD).
 - a. Original AROI is retained in field office case file.
 - b. Upload the final AROI into iManage according to directions provided by the SAC Investigative Support Branch.
- (2) Investigations Closed With Status Code of Closed – Referred (CLRF) or Closed – Management Review (CLMR). Applies to BOP and USMS “60 day” cases only.
 - a. Retain original AROI in field office case file.
 - b. Forward one copy of the AROI directly from the field office (via Field Office Form 2 – *SharePoint Forms: IG Manual*) to the component agency.
 - c. Upload the final AROI into iManage according to the directions provided by the SAC Investigative Support Branch.
- (3) Investigations Closed as Information to the Field Office File (CLRI). Applies to BOP and USMS “60 day” cases only.
 - a. Original AROI is retained in the field office case file.
 - b. Upload the final AROI into iManage according to the directions provided by the SAC Investigative Support Branch. The field office will submit a memorandum (Field Office Form 3 – *SharePoint*

Forms: IG Manual) directly to the component internal affairs office as documentation that the OIG investigation has been closed. Upload the memorandum into iManage.

207.11 Priority Cases. The Inspector General or INV Headquarters may designate any investigation as a “priority case.” Priority cases will be completed expeditiously, and if resource constraints exist, priority cases will be worked ahead of regular, non-priority investigations.

A. Types of Priority Cases. Priority cases usually fall under one of the following categories:

- (1) Significant Criminal Cases. Investigations that will have an impact on a national program of DOJ or a component (for example, FBI, DEA, or the Executive Office for U.S. Attorneys) or cases that, if proven, will have national as well as local implications, such as a major corruption investigation.
- (2) Attorney Cases. Any investigation, whether criminal or administrative, where a subject is a DOJ attorney.
- (3) Political Appointees or High-Level Officials. Any investigation where a political appointee, such as a U.S. marshal, is a subject or any investigation where a DOJ official at the Senior Executive Service level or above is a subject.
- (4) Other Sensitive or Unusual Cases. Includes sensitive investigations, such as certain civil rights cases, or situations where the matter under investigation or the crime committed is of an unusual nature. Field office SACs must discuss each case possibly falling under this category with the SAC, Operations Branch I or Operations Branch II, INV Headquarters, before designating it as a priority case.
- (5) Deputy Attorney General Briefed Cases. Any investigations that have been identified that the IG or the DIG will brief the Deputy Attorney General on a periodic basis.

B. Investigative Work Agreement. The OIG Form III-207/8 (Investigative Work Agreement for Priority Investigations) (*SharePoint Forms: IG Manual*) is required for all priority cases, unless the investigation has been substantially completed at the time it is designated a priority case. The SAC will coordinate with the responsible INV Headquarters SAC (that is, the SAC, Operations Branch II, for cases involving ATF, DEA, and FBI SAC, Operations Branch, for all other DOJ components, offices, boards, and divisions; and the SAC, Investigative Support Branch, if the case involves investigative activities requiring DOJ Office of Enforcement Operations approval) (see IGM III-250). When required, the case agent will prepare

the Work Agreement and submit it to his or her SAC/ASAC when the investigation has been designated a priority. Within 2 weeks of designating an investigation as a priority case, the SAC must forward the Work Agreement to the responsible INV Headquarters SAC.

- (1) The responsible INV Headquarters SAC must agree with the field office on the specific allegations to be addressed and the direction of the investigation. This agreement will be memorialized on the Investigative Work Agreement and in a statement included in IDMS under the case number.
- (2) The various sections of the Work Agreement must be completed in their entirety and are self-explanatory. However, the section entitled “Specific Allegations To Be Answered by the Investigation” deserves special attention. This is the most important section of the Investigative Work Agreement. It will eliminate any misunderstanding between headquarters and the field office about the investigative expectations in the case.

C. Reports of Investigation. Case agents will normally prepare ROIs for all completed priority investigations.

- (1) Except in unusual circumstances, AROIs are not an acceptable format for reporting priority investigations. The SAC, Operations Branch I, or the SAC, Operations Branch II, INV Headquarters, must approve in advance any priority case reported in any format other than an ROI.
- (2) The responsible INV Headquarters SAC and field office will confer regarding case reports at the conclusion of investigations and after reviewed reports are returned for additional investigative work or report revision. (An outline of the report review process is available on *SharePoint Forms: IG Manual*.)
 - a. At the conclusion of priority investigations, discussions will include findings, ROI or AROI format, and the report completion date.
 - b. After reports are returned for revision or additional investigative work, discussions will include revisions and the report completion date.

207.12 Interim ROIs.

A. When Required.

Interim ROIs are required only in the following circumstances:

- (1) when necessary to report the final results of investigation regarding nonfugitive subjects in multiple subject cases where one or more of the subjects are fugitives (see Section 207.15).
- (2) when the AIGI or DAIGI requests an interim ROI in complex cases of particular interest to headquarters.
- (3) when the field office SAC requires the preparation of an interim ROI when the SAC considers it beneficial to case management.
- (4) when requested by a prosecutor in criminal investigations (see Section 207.13).
- (5) when a special request for an interim ROI from an appropriate DOJ component has been approved by the INV Headquarters SAC of interest.

B. Distribution. The original interim ROI will be retained in the field office case file and will be uploaded into iManage according to directions provided by INV Headquarters. Copies of interim ROIs will be disseminated as follows:

- (1) For interim ROIs prepared for reporting the final results of investigation regarding nonfugitive subjects, INV Headquarters will provide a copy of the interim report to the component so that the component can initiate adverse action, if appropriate, against subjects for whom investigative action is complete, even though action is still pending regarding a fugitive subject.
- (2) The AIGI or DAIGI will determine the dissemination of copies of interim ROIs prepared at his or her request at the time of the request.
- (3) Copies of interim ROIs prepared at the request of the SAC or prosecutor will not be separately submitted to headquarters but will be attached as an exhibit to the final ROI or AROI reporting the closing of the investigation. (INV Headquarters will disseminate a copy of the final report with exhibits to the component after the investigation is closed.)

207.13 Prosecution Reports.

A. When Required.

Case agents will prepare a prosecution report in a criminal case whenever the responsible prosecutor requests it.

- (1) The prosecution report will usually be prepared as an interim ROI. SACs have the latitude, however, to prepare a presentation for prosecution in any format or style conforming to the reasonable request of the prosecutor. The

request for prosecution or confirmation of acceptance must be documented, however, even if only by a memorandum from the SAC to the appropriate U.S. Attorney.

- (2) If a prosecution report is written in a format other than an ROI or interim ROI, the relevant results of investigation predicated the prosecution request must be included in a subsequent ROI.

B. Distribution.

- (1) Field offices will forward ROIs prepared as prosecution reports and other forms of prosecution reports directly to prosecutors.
- (2) Do not submit a prosecution report copy separately to headquarters. Attach the report copy as an exhibit to the final ROI or AROI used to report the closing of the investigation.

207.14 Auxiliary Investigations. During the course of an investigation, if it becomes necessary to conduct an interview or obtain information in an area covered by another field office, a request for an auxiliary (AUX) investigation will be prepared. The use of an AUX investigation will be the rule rather than the exception.

A. Requests for AUX Investigations. The controlling (requesting) office SAC will request an AUX investigation by memorandum or formal e-mail to the SAC of the office being requested to conduct the investigation (receiving office).

- (1) The controlling office will make available, through IDMS or attachments to the AUX request, all the necessary background information an agent will need to conduct the requested AUX investigation effectively.
- (2) The controlling office will clearly state in the AUX request exactly what is being requested. Avoid general statements, such as “conduct interview of suspect.” Furnish enough detail to provide the interviewing agent with a thorough understanding of the purpose of the interview. To whatever extent possible, identify specific questions to be asked. If handwriting exemplars or other evidentiary items are to be obtained, specify the precise format or form in which the evidence is needed.
- (3) In complicated priority investigations, if either field office SAC determines that it would be more practical or expeditious to have an agent from the controlling (requesting) office conduct interviews or gather evidence in an area covered by another field office, the SAC of the controlling office and the SAC of the office where the work is to be done will consult before any action. Under no circumstances shall an agent from one field office travel to

another field office district without the prior concurrence of both affected field office SACs and the INV Headquarters SAC of interest.

- B. Case Management. The receiving office will create an AUX case in IDMS under the same OIG number as the controlling office.
- (1) The receiving office will expeditiously work an AUX investigation and should complete the investigation within 30 days of receipt. If the receiving office cannot complete the requested investigation within 30 days, a status report in the form of a memorandum or formal e-mail message, explaining the delay, must be submitted to the controlling office.
 - (2) When conducting an AUX investigation, if information is developed that indicates the need for additional investigation in yet a third field office, notify the controlling office. The controlling office will evaluate the developed information and, if deemed necessary, will request that an AUX investigation be conducted by the third office.
- C. AUX Report. The results of AUX investigations will be reported to the controlling office by a transmittal memorandum or formal email message from the receiving office SAC to the controlling office SAC. Attached to the transmittal memorandum or formal email will be exhibits with the relevant MOIs. The transmittal memorandum or formal email message with exhibits/MOIs will serve as the closing report for the AUX investigation. The receiving office will then close the AUX investigation in IDMS.
- D. Distribution.
- (1) The original transmittal memorandum and closing memorandum or formal email with copies of the exhibits/MOIs reporting the results of an AUX investigation will be uploaded into iManage by the receiving office.
 - (2) The receiving office will submit the closing memorandum or formal email with the original exhibits/MOIs to the controlling office. Submit all relevant original written affidavits, original records obtained, and original handwritten notes with the copy of the AUX memorandum to the controlling office.
 - (3) Do not submit copies of AUX memoranda or formal email message to headquarters.
- E. Controlling Office Actions When Closing Predicating Case. When closing the predicating investigation, the controlling office will report in their ROI or AROI significant information furnished in the AUX memorandum or formal email. The

controlling office will attach the AUX memorandum or formal email (including any supporting documents) as an exhibit to the closing ROI or AROI.

207.15 Fugitive Status.

- A. Fugitive. The subject of an OIG investigation who fails to appear for a scheduled federal judicial proceeding following an arrest or indictment and for whom a warrant has been issued by the court for failure to appear or flight to avoid prosecution is considered a “fugitive.” The USMS has primary responsibility for apprehending fugitives.
- B. Wanted Person. An OIG subject for whom an arrest warrant has been issued but who has not yet been arrested or indicted is considered a “wanted person” and is not a “fugitive.” The investigative agency that obtains the arrest warrant, not the USMS, has primary responsibility for apprehending wanted persons. An OIG investigation will not be placed in “fugitive status” for a wanted person.
- C. OIG/Field Office/Agent Responsibility.

The OIG will work jointly with the USMS to locate and arrest OIG fugitives.

(b) (7)(E)



- D. Case Management. The original investigation of the substantive offense will remain open until the fugitive has been apprehended or the pending judicial action on the substantive charge has been resolved.
 - (1) To enable a component to take appropriate administrative action, case agents must report the investigative results concerning any nonfugitive subject in a multiple subject case by interim ROI (see Section 207.12) as soon as the investigation pertaining to the nonfugitive subjects or any pending judicial action against that subject is complete.
 - (2) Change the IDMS status code for an investigation with a fugitive subject to “Open-Fugitive” (OPFG).

(3) The SAC/ASAC will ensure that cases with fugitives are promptly and continuously investigated and that the activity is promptly and properly reported by MOI. Fugitive cases require investigative activity and reporting at least every 120 days.

(4) Agents must also keep fugitive case status information current in IDMS.

E. Documentation.

(1) The case agent will prepare an MOI to document the issuance of the fugitive warrant and placement of the case in a fugitive status.

(b) (7)(E)

A large black rectangular redaction box covers the text in this section. The text "(b) (7)(E)" is visible in red at the top left corner of the redaction.

(3) Copies of pertinent documents, including NCIC warrant entries, Apprehension Investigation Requests, and copies of any “stops” or lookouts placed with local, state, and federal agencies, will be documented by MOI and placed in the case file and uploaded to iManage.

(b) (7)(E)

A large black rectangular redaction box covers the text in this section. The text "(b) (7)(E)" is visible in red at the top left corner of the redaction.

F.

(b) (7)(E)



- G. Subsequent Information. The case agent (or the FOFC) will forward any subsequently developed relevant information to the USMS via memorandum. The memorandum will at minimum contain the following:
- (1) OIG case file number;
 - (2) case file title;
 - (3) name of fugitive; and
 - (4) additional investigative information or leads.
- H. Arrest of the Fugitive.
- (1) When an OIG agent arrests a fugitive subject, he or she will create a separate second Arrest Record and Judicial Action Record for that subject in IDMS.
 - (2) Report the arrest of the fugitive by an MOI. Change the IDMS case status code from “OPFG” back to “OPJP.” Complete the IDMS Judicial Action Record for the fugitive offense as soon as that charge is adjudicated.

- (3) When the court adjudicates the original charge upon which the fugitive subject's original arrest/indictment was predicated, also complete that Judicial Action Record in IDMS.
 - (4) Report the disposition of judicial action regarding both arrests in the closing ROI. The disposition may be reported by a closing AROI if all other pertinent results of the investigation have been previously reported by interim ROI.
 - (5) All required arrest history information for both arrests will be obtained and retained in the office case file folder, disseminated as appropriate, and properly recorded in IDMS.
- I. Inactive Status. The SAC may authorize placing the case in an "inactive" status after 1 year in a fugitive status if all investigation in the case other than the adjudication of the fugitive subject's original arrest/indictment has been completed and reported, diligent investigation and all appropriate lookouts have failed to locate the fugitive, and no viable investigative leads remain.
- (1) The case agent will prepare an MOI reporting updated investigative efforts and documenting the SAC's authorization of inactive status.
 - (2) "Inactive" fugitive status requires that an MOI be prepared no later than 1 year from the date of the MOI placing the investigation in an inactive status.

J.

(b) (7)(E)



(b) (7)(E)



207.16 Sworn Statements.

See also IGM III-226 for related information regarding OIG interview procedures.

- A. Objectives and Strategy. The objective is to obtain the subject's or witness's version of the incident or allegations under investigation. A self-serving statement is generally not useful in resolving allegations. Adequate thought and preparation are essential to an effective interview. Rather than just asking formulaic questions, agents need to think strategically before and during the interview regarding the issues:

(b) (7)(E)



(b) (7)(E)

- B. Authority. OIG Special Agents are authorized to administer oaths and request information under oath, pursuant to the Inspector General Act, title 5 U.S.C. app. § 6(a)(5).
- C. Non-Criminal Cases. Agents will take sworn statements (written affidavits or audio or audio-video recorded) from persons who have direct evidence concerning the allegations in investigations that originate as non-criminal cases or in criminal cases in which prosecution has been declined. This includes subjects as well as relevant witnesses.
- (1) Sworn statements in non-criminal cases are especially important because they are generally admissible as evidence in administrative proceedings if the witness is not available to testify.
 - (2) Sworn statements can be essential to the component agency when a subject employee chooses to have a case decided by a third party, who will have only the record, that is, the investigative report and exhibits, on which to base a decision.
- D. Criminal Cases. Once a case has been presented for criminal prosecution, agents will follow the prosecuting attorney's guidance in determining whether sworn statements shall be obtained during any subsequent interviews. Sworn statements of witnesses may become problematic at trial, particularly when grand jury testimony is also involved.
- E. Sworn Statement Formats: Written Affidavit. A sworn statement normally will be a handwritten or typed, signed declaration or statement of fact, made under oath before affixing the affiant's signature — that is, a written narrative affidavit. Prepare the written affidavit at the time of the interview, using OIG Form III-207/3 (Affidavit) (*SharePoint Forms: IG Manual*).
- (1) The preferred method of taking a sworn statement is an affidavit written in narrative format, prepared by the interviewing agent. However, if the interviewee refuses to provide a statement unless the interviewee writes his or her own affidavit, then the agent may allow the interviewee to do so. Before the affidavit is sworn to, the agent must assure that all relevant issues are addressed and that the interviewee is dissuaded from providing self-serving statements when contradictory evidence exists.
 - (2) The items to be completed on the affidavit form are self-explanatory. The following items, however, should be given special attention:

- a. Oath. Before taking the affidavit, the agent taking the statement will administer the oath cited on the first page of the affidavit form. The affiant will raise his or her right hand in affirmation, and the agent will read the oath contained in the opening paragraph.
 - b. Affiant's Initials. After having been afforded an opportunity to read and make necessary changes to the statement, the affiant will initial the lower right corner of each page and initial each erasure, strikeover, cross out, or other change made in the body of the affidavit before attesting to its content.
 - c. Affiant's Signature. The affiant will sign the last page of the affidavit above the line marked "Affiant's Signature."
 - d. Investigator's Signature — Jurat. The agent administering the oath will complete the authentication and sign the Jurat section at the end of the affidavit.
- (3) Carefully review the affidavit upon completion, to make sure all errors are identified, corrected, and initialed and to assure that the interviewee has initialed each page and signed the affidavit.
 - (4) The original written affidavit will be handled with its evidentiary value in mind; however, it need not be secured with the evidence custodian.
 - (5) If necessary, a working copy of the affidavit may be made. The copy must be marked as such. Care must be taken in handling the copy to safeguard it from unauthorized disclosure.
 - (6) If a handwritten affidavit is taken, a verbatim, typed copy will be prepared and included with the handwritten version as an exhibit to the ROI. This will ensure ease of reading of the affidavit by recipients of the report.
- F. Sworn Statement Formats: Audio or Audio-Video Recorded Affidavit. Agents may take an audio or an audio-video recorded statement. All subject interviews should be recorded (unless a specific reason for not doing so is provided to INV Headquarters prior to the interview, i.e., the prosecutor in a criminal case has requested that the interview not be recorded). Custodial interviews of individuals following arrest, but prior to an initial appearance before a judicial officer, in a place of detention with suitable recording equipment will be recorded in accordance with the guidelines in section G below.

Significant witness interviews should be audio or audio-video recorded. The following guidelines will be adhered to when taking audio or video recorded statements:

- (1) Test the recording equipment before the interview to make sure that it is working properly and that you are familiar with the operation of the equipment. If possible, set up the recording equipment in the interview room ahead of time.
- (2) Consider the estimated length of the interview vis-à-vis the time limits of the tapes. Have additional tapes and batteries readily available.
- (3) Remember that everything you say will be recorded.
- (4) Read and record the following preamble at the beginning of the interview session:

“My name is _____. I am a Special Agent with the U.S. Department of Justice, Office of the Inspector General, _____ Field Office. This interview is being conducted as part of an official investigation. Today’s date is _____. The time is _____. This interview is being conducted at _____. Also present is/are _____ (identify all persons present, including union representatives, attorneys, and other agents).”
- (5) Advise the interviewee that he or she “is here today as a (subject or witness) to answer questions in an official OIG investigation regarding allegations of _____.” Read the appropriate OIG warnings form (if applicable) and allow the interviewee and his or her representative time to read it.
- (6) Before making any other statement on the recording, place the interviewee under oath in the same manner prescribed for a written affidavit.
- (7) Conduct the interview. The first part of the recorded interview will include the interviewee’s identifying information as outlined in sections 5 through 18 of the OIG affidavit form (SharePoint Forms: IG Manual).
- (8) Indicate on the recording any request for a recess during the interview. Also note the time, duration, and reason for the recess. Remember to turn the recorder back on when the interview resumes.
- (9) Do not allow the subject or his or her representative to tape record the interview. The OIG audio or video recording will be the only recording of an interview.
- (10) When you have completed your questioning, ask the interviewee if there is anything he or she would like to add.

- (11) Inform the interviewee on the recording that the interview is concluded. Note the concluding time and turn off the recording device.
 - (12) Handle an original recording as if it has evidentiary value in the same manner as a sworn affidavit. However, the recording does not need to be secured with the evidence custodian.
 - (13) If necessary, agents may make a working copy of the recorded statement. The copy will be marked as such.
 - (14) Prepare a transcript of the interview as soon as is feasible. Transcripts will only be prepared under the direction of OIG personnel.
 - (15) The agent taking the sworn statement will review and certify the interview transcript as being an accurate representation of what is on the recording.
 - (16) OIG employees will take care in handling working copies of recordings and transcripts to safeguard them from loss or unauthorized disclosure.
- G. Recording Custodial Interviews. Agents will comply with the DOJ Policy Concerning Electronic Recording of Custodial Statements in Appendix B. Although the DOJ policy does not specifically address the OIG, the contents of the policy statement are applicable to OIG agents by incorporation to this chapter.
- H. Copies. Do not provide copies of statements to interviewees or their representatives. The person making the statement may obtain a copy by submitting a written Freedom of Information Act request through prescribed channels. The copy will not normally be provided until after the case is closed. However, if a person is being interviewed a second time and requests to review a prior statement, the agent will allow the person to do so. Copies of warning forms signed during the interview should be provided to interviewees or their representatives, if requested.
- 207.17 Documenting Statements. Agents will document in an MOI any interview or declaration of fact that is not written in an affidavit or audio or audio-video recorded.
- A. Documents. Any unsworn testimony received in document form, such as a memorandum or letter, will be summarized in an MOI and attached to the MOI. The MOI will also contain an explanation of when, how, and from whom the document was received.
 - B. Refusal To Be Placed Under Oath. Agents will document in an MOI interviews of individuals who refuse to be placed under oath or to provide a signed, sworn statement. Document the individual's refusal to be placed under oath or to give a signed, sworn statement as well as the substance of the interview in the MOI. DOJ regulations require all DOJ employees to cooperate with the OIG and to respond to

questions posed to them during an investigation upon being informed that their statements will not be used to incriminate them in a criminal proceeding (28 C.F.R. § 45.13). In addition, BOP policy provides that BOP employees are required to give a statement under oath in administrative investigations.

207.18 Special Procedures Regarding the FBI.

A. Notification to Subjects.

- (1) The OIG will provide FBI employees who are the subjects of administrative misconduct investigations written notice within 30 days of the initiation of an administrative investigation.
- (2) The OIG will not provide written notification to subjects of criminal investigations.
- (3) If the OIG opens an investigation based on criminal allegations that are subsequently declined for prosecution, the OIG must inform the FBI subject of any continuing administrative inquiry within 30 days of the declination.
- (4) The OIG will make the required notification of an investigation initiation to the FBI employee through the FBI Inspection Division, using OIG Form III-207/11 (Notification) (SharePoint Forms: IG Manual), except when case considerations indicate against this notification.

B. Nondisclosure Agreement for Attorneys in FBI Cases. In parallel with the FBI's practice of requiring an attorney representing an FBI employee to sign a confidentiality and nondisclosure agreement in regard to FBI information revealed during an investigation, OIG investigators will employ OIG Form III-207/9 (Agreement to Maintain Confidentiality and Non-disclosure of Information) (*SharePoint Forms: IG Manual*). The form is an agreement between the OIG and a subject's attorney.

207.19 Closing Investigations.

A. Criteria. Case agents will submit investigations for closing only when the investigation is complete — that is, when all investigative leads have been exhausted and all administrative, as well as criminal, allegations are addressed, as directed by INV managers.

- (1) Administrative Cases. A declination of prosecution is not sufficient reason to close an investigation unless all administrative allegations have been addressed and properly reported. As a result of the OIG investigation, there should be no need for the component to conduct any additional investigation

or interviews before taking administrative action. However, the OIG may close a case before the component completes administrative action.

- (2) Criminal Cases. Cases resulting in criminal prosecution may not be closed until after the criminal adjudication process is complete through sentencing; all required judicial documents have been obtained and placed in the case file; fingerprint cards/R-84 (Final Disposition Report) forms have been submitted to the FBI; and all evidence has been properly disposed of (see IGM III-234). All R-84 forms must be uploaded to iManage.

B. Sixty-Day Cases. “Sixty-day cases” are the lone exception to the above criteria.

- (1) Certain component agencies (presently only BOP and USMS) with internal affairs offices that can address administrative issues have agreed to address unresolved administrative allegations in OIG investigations if:
 - a. the OIG has resolved all the criminal issues raised by the complaint, and
 - b. the SAC approves and signs the closing report of investigation not more than 60 days after the OIG received the original complaint.
- (2) SACs are authorized to close an investigation before it is complete and refer any unresolved administrative issues to the component’s internal affairs or internal inspections unit when the above conditions are met.
- (3) The field office will close investigations with remaining administrative issues as “Referred” (IDMS code “CLRF”) or “Management Review” (IDMS code “CLMR”).
- (4) The field office will send the closing report directly to the BOP or USMS internal affairs office.
- (5) If the OIG investigation proves the complaint to be without substance and if the SAC determines that no further action is warranted by either the OIG or the component, the case will be closed as “Information to the File” (IDMS code “CLRI”), provided that less than 60 days has elapsed since the OIG received the initial complaint.
- (6) In all cases, SACs will investigate cases quickly and efficiently, with a judicious use of resources and consideration of all DOJ resources when managing cases. SACs are not encouraged to refer the administrative aspects of an investigation back to a component where total completion of the investigation by the OIG would require only minimal additional time and resources.

- C. Reports. When an investigation is to be closed, the case agent will prepare an ROI or, if appropriate, an AROI, with all exhibits attached.
- (1) The case agent will submit the completed report to the ASAC/SAC for approval. The case agent also will ensure that the office case file folder is assembled in compliance with OIG requirements (see Section 207.7) and that the report is uploaded into iManage.
 - (2) The ASAC/SAC will submit the completed report to INV Headquarters and ensure that the report's submittal is in the ROI Tracking System.
- D. iManage. All case-related investigative documents will be created directly in IDMS or imported into iManage. Grand jury and classified documents are not to be created in or imported into iManage. Any voluminous documents collected during an investigation (for example, bank records, telephone records, and so forth) are not required to be imported unless they are attached to an MOI and are pertinent to resolving and reporting the investigative matter or would otherwise be required to be retained with the case file in accordance with records management requirements.
- (1) Although creating MOIs and ROIs in iManage is encouraged, once an MOI or ROI has been completed, draft documents must be deleted. When a case is closed, the field office managers will review iManage and ensure that no draft documents have been retained and that all final documents, including all MOIs generated during the investigation, have been uploaded. The documents should be the final signed documents.
 - (2) Documents loaded into iManage must be given easily recognizable file names, enabling persons not familiar with a case to locate specific documents. For example:
 - [Document Type] [Name] [Date of Document or Activity].pdf
 - Plea with Statement of Fact for Masahiro Takahashi 01-10-18.pdf
 - MOI for Robert T. Lawless 12-10-17.pdf
 - Judgment and Commitment for Rebecca M. Jones 01-10-18.pdf
 - Plea Agreement for Jorge A. Hernandez 09-30-17.pdf
 - Arrest Warrant and Indictment for Harold Z. Smith 11-11-17.pdf
 - Superseding Indictment for Elizabeth L. Parker 01-20-18.pdf
 - 2018-001234 ROI – William B.Thompson.pdf
 - Civil Judgment for Wilma W. Wilson 08-22-18.pdf
 - R-84 for Anthony C. Washington 04-05-18

All documents and exhibits uploaded into iManage as part of an AROI or ROI must adhere to current guidance provided by INV Headquarters.

- E. IDMS. The case agent must complete all appropriate IDMS fields, including the disposition field for each allegation (IDMS offense code) for each subject. The case agent and the approving supervisor will review all IDMS data as part of the final review of the case before closing. The final updated IDMS printout will be included in the office case file folder.
- F. Supervisory Approval.
- (1) The supervisor's signature on the closing report is his or her certification that the report, field office case file, and all IDMS data are complete, current, and correct. The supervisor should use the Case Review -- Supervisor's Checklist (SharePoint Forms: IG Manual) and the Case Review Record (SharePoint Forms: IG Manual) to assist in assuring that all appropriate items have been reviewed before closing the investigation.
 - (2) Investigations are considered closed on the date INV Headquarters approves the final ROI or AROI for distribution to the component or as per guidance provided by INV Headquarters.
- G. Exoneration Letters. When an OIG investigation completely exonerates the subject of any wrongdoing, the field SAC shall identify the case to the responsible INV Headquarters SAC and may recommend that an exoneration letter be prepared. All exoneration letters will be prepared at INV Headquarters, and the responsible INV Headquarters SAC must obtain the agreement of the relevant component that an exoneration letter is appropriate before disseminating the letter.

207.20 Procedural Reform Recommendations. Agents and supervisors will review each completed OIG investigation with a view toward identifying any systemic weaknesses in component agency programs, policies, procedures, or practices that made commission of the offense at issue in the investigation easier. If systemic problems and a potential solution are identified, a Procedural Reform Recommendations (PRR) will be prepared. See III-210 and the current *PRR Format and Style Standards Guide* issued by headquarters as posted in SharePoint for additional guidance.

- A. Field Office Responsibilities. The case agent will normally prepare the PRR. The ASAC and SAC will carefully review the completed PRR to assure a high quality product.
- B. Distribution. The PRR will be submitted to INV Headquarters with the closing report of investigation. Further dissemination of the PRR is the same as for the closing ROI or AROI. Headquarters management will consult with the Front Office to determine whether the PRR will be posted to the OIG public website.

207.21 Monitored Referral Investigations (IDMS Classification "R").

- A. Responsibility. The SAC, Operations Branch I, or SAC, Operations Branch II, INV Headquarters (depending on the component involved), will decide which complaints to refer to components for investigation and reporting of the results back to the OIG. He or she will then forward the complaint to the appropriate component for investigation.
- (1) Field office SACs may recommend to the SAC, Operations Branch I, or the SAC, Operations Branch II, that appropriate complaints be classified as monitored referrals. However, the final decision rests with the SAC, Operations Branch I, or SAC, Operations Branch II.
 - (2) The SAC, Operations Branch I, and the SAC, Operations Branch II, are responsible for assuring that the appropriate IDMS entries are made to create, monitor, and close referred investigations. Final reports received from DOJ components will be uploaded into iManage.
- B. Monitoring Methods. The SAC, Operations Branch, and SAC, Operations Branch II, will monitor the quality and timeliness of investigations referred to the components by:
- (1) receiving and reviewing individual investigative reports of completed monitored referral cases and, if necessary, requesting additional information or investigative action; and
 - (2) requiring periodic summary status reports from the component regarding all pending monitored referrals assigned to that component.
- Field office SACs also may request to review a particular completed monitored referral report through the SAC, Operations Branch I, or SAC, Operations Branch II, INV Headquarters. The field SAC must articulate the reason for the request (for example, a field office receives a new allegation against the subject of a prior monitored referral investigation).
- C. Oversight Responsibility. The SAC, Operations Branch I, and SAC, Operations Branch II, will ensure that monitored referral investigations conducted by the components are thorough, objective, and timely. They will ensure that reports of investigation from the components at minimum include the following:
- (1) a summary of the allegations;
 - (2) the scope of the investigation, including the names and identities of all relevant persons interviewed;
 - (3) significant investigative findings;

- (4) any and all information that either supports or discredits the allegations; and
- (5) the results of any judicial actions (such as off-duty arrests) and any administrative or corrective actions proposed or taken by the component.

207.22 Initiatives.

- A. Definition. Proactive investigative actions conducted to identify criminal or civil misconduct or administrative issues that adversely affect DOJ's operations, security, systems, assets, or mission. Initiatives will be based on received or developed information indicating that misconduct might exist within a program, issue, or entity but will not initially contain sufficient predication to warrant opening an OIG investigation.
- B. Opening an Initiative.
 - (1) Opening an initiative requires INV Headquarters approval. All requests will be made via memorandum from the field office SAC to the Deputy Assistant Inspector General for Investigations, INV Headquarters, with a copy to the appropriate SAC (Operations Branch I or Operations Branch II, INV Headquarters).
 - (2) The memorandum will fully describe the received or developed information that the field office believes warrants review by INV and why the matter should be handled as an initiative as opposed to an investigation. The goals of the initiative must be clearly stated along with a description of the resources – both field office and INV Headquarters – needed to review the matter.
- C. Administrative Procedures.
 - (1) IDMS Code OPIN will be used to open an initiative and Code CLIN will be used to close an initiative.
 - (2) An initiative will not be subject to the INV 180-day timeliness goal but will be reviewed every quarter during SACs calls, and a joint determination will be made to continue investigating the matter or to close it.
 - (3) If sufficient predication is developed during the initiative to warrant investigation of misconduct by a specific subject, a separate investigation will be opened. Examination of misconduct by a specific subject will not be conducted within an initiative.
 - (4) If a decision is made to close the initiative, an AROI may be used to describe the investigative efforts conducted during the initiative and the results of

those efforts. The memorandum that proposed the initiative becomes a part of the file. A copy of the closing AROI is provided to INV Headquarters – no copies will be provided outside of the OIG.

207.23 Use of (b) (7)(E) in BOP Investigations. (b) (7)(E)
[Redacted]

A. OIG (b) (7)(E) Compliance Manager. The SAC, Operations Branch I, INV Headquarters, is designated as the OIG individual responsible for liaison with the BOP concerning (b) (7)(E) issues and for ensuring OIG compliance with the terms and conditions of the memorandum of understanding between the OIG and BOP concerning OIG use of (b) (7)(E) (Appendix A).

B. Authorized Communication Systems. (b) (7)(E)
[Redacted]
[Redacted]
[Redacted]
The SAC, Operations Branch I, INV Headquarters, will provide the AIGI with a memorandum designating the computers and locations authorized for (b) (7)(E) access. Remote access to (b) (7)(E) is prohibited.

C. Authorized Users. Authorized users are only those OIG employees with (b) (7)(E) accounts. Accessing (b) (7)(E) by unauthorized users is prohibited. Users are authorized as follows:

- (1) The SAC, Operations Branch I, INV Headquarters, will submit an OIG user account request to the BOP;
- (2) The BOP will establish the account and then provide the user with an initial password;
- (3) The SAC, Operations Branch I, INV Headquarters, will provide users with a current copy of the (b) (7)(E) rules. The user must read the rules and agree to abide by the rules by signing the (b) (7)(E) use form prior to accessing (b) (7)(E)
- (4) The SAC, Operations Branch I, INV Headquarters, will forward the user's signed (b) (7)(E) use form to the BOP and retain a copy; and
- (5) The SAC, Operations Branch I, INV Headquarters, will recertify to the BOP authorized users annually.

- D. Deactivation of Users. The SAC, Operations Branch I, INV Headquarters, will notify the BOP that a user is no longer authorized to access (b) (7)(E) as follows:
- (1) immediately upon the separation of the user (for example, involuntary termination, transfer, resignation);
 - (2) immediately upon suspected misuse by a user;
 - (3) immediately upon suspected compromise of a user password; and
 - (4) within 1 day of a user no longer needing access to (b) (7)(E)
- E. Authorized Use of (b) (7)(E) Users are authorized to access (b) (7)(E) in order to develop leads and for other purposes related to official OIG Investigations Division investigations. Users must use their best efforts to limit the information obtained from (b) (7)(E) to that information that is immediately useful in connection with the specific matter prompting a particular query. Best efforts in this context include, but are not limited to, only as much information as is reasonably available to users in framing and narrowing a query. When making queries concerning specific persons or entities (subjects), users shall use identifying information related to those subjects in order to eliminate, insofar as possible, the retrieval of information not related to the subjects. Users will use their best efforts to obtain and maintain only that information that is of value in connection with the specific matter prompting the query.
- F. Prohibited Use of (b) (7)(E) Users are prohibited from accessing and sharing (b) (7)(E) information as follows:
- (1) for another federal, state, or local agency (information may be shared when working a case jointly);
 - (2) for non-Investigations Division OIG personnel (except in support or review of an authorized investigation);
 - (3) for non-official reasons; and
 - (4) for any reason not covered by paragraph E above.
- G. Recordkeeping. (b) (7)(E) users will complete the data fields in the (b) (7)(E) Usage Tracking Log in SharePoint concurrent with each search session.
- H. Safeguarding (b) (7)(E) Information. Users will ensure that BOP data and records created via access to (b) (7)(E) will not be duplicated or re-disclosed within or outside of the OIG, except as authorized by law or when essential to the conduct of an investigation. Users will promptly destroy all documents or summaries obtained

or generated that do not contain information of value to a specific investigative query of (b) (7)(E) data and documentation will be handled in accordance with IGM Volume I, Chapter 222, "Standards for Safeguarding Sensitive But Unclassified Information."

- I. Security Incidents. The SAC, Operations Branch I, INV Headquarters, will immediately contact BOP concerning all security incidents that could affect (b) (7)(E) access connections, BOP systems or networks, or BOP data.

207.24 Special Procedures Regarding the Management of Investigations of Allegations of Sexual Abuse in Confinement Settings.

A. Training.

- (1) All investigations of sexual abuse in confinement settings, including BOP and USMS facilities and contract facilities, will be conducted by Special Agents who have completed special training in sexual abuse investigations. Training is currently available on SharePoint. The training taken by personnel will be documented and recorded by the INV Investigative Support Branch.
- (2) For additional resources and educational materials from the National Resource Center for the Elimination of Prison Rape, visit www.prearesourcecenter.org.

- B. Standards. The investigating agents will gather and preserve direct and circumstantial evidence, (b) (7)(E)

[REDACTED]

C. Victim Safety.

- (1) The first priority at all times must be the safety of the inmate victim.

(b) (7)(E)

[REDACTED]

Although inmate housing assignments are the responsibility of the component, OIG agents should be aware of relevant regulations when working with the component.

- (2) PREA victim safety protocols call for the separation of the victim and a staff subject; therefore, Office of Enforcement Operations (OEO) approval generally will not be granted for any operation involving face-to-face contact

between the victim and the staff member. Under no circumstances will unmonitored fixed cameras be installed and operated by the OIG in "private" areas (that is, interior offices) where sexual activity is suspected. During joint investigations with other agencies, it is the responsibility of the case agent to verify that the use of inmates and any technical operations are authorized, regardless of which agency submits the use of prisoner request to OEO.

- D. Victim Advocates. Requests for victim advocates will be honored. (See IGM 111-226, Interview Procedures.)
- E. Use of Polygraph. No inmate who alleges sexual abuse will be required to submit to a polygraph examination as a condition for proceeding with an investigation of the allegation.
- F. Refusal of Victim to Cooperate. The refusal of a victim to cooperate with the investigation will not be the sole basis for terminating an investigation, provided that sufficient evidence exists or may be developed from other sources to build a credible criminal or administrative case.
- G. Departure of Subject or Victim. The departure of the alleged abuser or victim from the employment or control of the facility or agency will not provide a basis for terminating an investigation.
- H. Proving Contact. Investigating agents will pursue available leads to detect any inappropriate contact between the staff member and the inmate victim, including e-mails, letters, texts, telephone calls, social media, photographs, financial transactions, and so forth. Investigators will attempt to identify aliases, alias e-mail accounts, and third parties used to further contact between the staff member and the victim. Agents will utilize subpoenas as necessary to further these goals.
- I. Presentation for Prosecution. All investigations with evidence that appears to support criminal prosecution will be presented to the U.S. Attorney's Office with jurisdiction. No compelled interviews will be conducted in connection with such a case without the concurrence or a prosecutorial declination from an Assistant U.S. Attorney.
- J. Administrative Investigations. All investigations in which prosecution was declined or resulted in a misdemeanor conviction without the voluntary resignation of the subject will be completed administratively. The component will be provided with a report of investigation that explains the basis for any findings of administrative violations and includes citations to the respective policies. The report will include compelled interviews of the subjects unless the subjects admitted to the violations during voluntary interviews memorialized with affidavits or audio recordings.
- K. Processing Non-DOJ PREA Allegations. Processing is prescribed in IGM III-205.12A and B and as follows:

- (1) Disposition. Under 28 C.F.R. § 115.71, all allegations of sexual abuse or sexual harassment of inmates by staff members, contractors, or volunteers will be investigated promptly, thoroughly, and objectively, including allegations received from third parties and anonymous reports. If initial review or preliminary investigation of the allegation determines that it is unlikely to result in a criminal prosecution, the SAC or ASAC of the field office of jurisdiction may request that the allegation be referred to the component for investigation. The referral will be made by the relevant INV Headquarters Operations Branch, in consultation with the field office. All such referrals will be monitored referrals unless no additional investigative steps are necessary or if the conduct, as reported and if true, would not amount to a serious administrative violation, in which case a management referral may be considered. All non-DOJ PREA allegations may be assigned a disposition by the SAC or ASAC of the field office of jurisdiction. See also IGM III-205, Appendix D, for definitions of sexual abuse and harassment terms in the Prison Rape Elimination Act (PREA).
- (2) IDMS and iManage.
 - a. Allegations that fit the PREA definition of sexual abuse or harassment that are state and local issues not related to DOJ will be referred by the office of receipt to the Civil Rights Division. Use the complaint code 498 (non-DOJ Issue); check the PREA box in IDMS; and assign a disposition of “X.”
 - b. Allegations that fit the PREA definition of sexual abuse or harassment that are non-DOJ federal issues will be referred by the office of receipt to the respective federal agency’s OIG (for example, Department of Homeland Security OIG). Use the complaint code 498 (non-DOJ Issue); check the PREA box in IDMS; and assign a disposition of “X.”

207.25 Conflict of Interest Investigations. The Ethics in Government Act, 5 U.S.C. appendix sections 101-105, requires concurrent notifications to the Office of Government Ethics (OGE) when any matter involving a potential violation by an executive branch employee of 18 U.S.C. sections 203, 205, 207, 208, or 209, is referred to DOJ for prosecution.

- A. Upon Referral to Prosecutor. Upon referral to the prosecutor, the case agent, or other designated field office staff, must complete Part 1 of OGE Form 202 (Notification of Conflict of Interest) and submit the form via email to referrals@oge.gov. OGE Form 202 is available on *SharePoint Forms: IG Manual*.
- B. Disposition of Referral When Case is Closed. The case agent, or other designated field office staff, must complete Part 2 of OGE Form 202 and submit the form via email to referrals@oge.gov after both of the following events have occurred:

- (1) the case is either declined, prosecution has begun and it has become a matter of public record, or the case has been settled through formal agreement; and
 - (2) the investigation of the matter has been concluded.
- C. When Adverse Findings Have Been Made. The case agent, or other designated field office staff, may satisfy the request for additional information regarding adverse findings by providing OGE with a link to the Summary of Investigative Findings posted on the OIG's public website.

APPENDIX A


**Memorandum of Understanding Between the
Office of the Inspector General and Federal Bureau of Prisons
(October 22, 2013)**

within the investigative jurisdiction of the OIG. Such purpose shall not include use by the OIG in conjunction with the OIG's non-investigatory authority, such as for its audit functions.

II. PURPOSE AND SCOPE:

A. This MOU is intended to establish responsibilities and procedures for authorized OIG investigative staff to obtain secure access to (b) (7)(E) through (b) (7)(E) solely on behalf of OIG and not on behalf of any other person or agency, and solely for the purpose of conducting investigations of matters that fall within the investigative authority of the OIG.

B. This MOU is intended to cover access to (b) (7)(E) only. This MOU does not provide OIG with any decision-making authority or control over application changes. (b) (7)(E)



C. This MOU shall not affect any pre-existing relationship or obligation between the parties on any other subject.

III. RESPONSIBILITIES:

A. BOP shall:

(b) (7)(E)



(b) (7)(E)



B. OIG shall:


1. Appoint a security manager responsible for interfacing with the BOP regarding this MOU and ensuring that authorized OIG users comply with the terms and conditions of this MOU and signed Rules.

(b) (7)(E)



3. Verify that approved OIG investigative staff users satisfy appropriate security requirements, thereby entitling them to become authorized OIG users for purposes of this MOU, and re-certify user lists annually for continued access.

4. Distribute to authorized OIG users a copy of the current Rules and obtain signatures from each authorized OIG user agreeing to abide by the Rules (b) (7)(E)



(b) (7)(E)



8. Immediately report to BOP all security incidents that could affect the access connections, BOP systems or networks and/or BOP data, in accordance with DOJ computer security policies. OIG shall communicate to BOP/TFB any outages or system problems. However, OIG acknowledges that outages and system errors may occur and there may be times when the system is unavailable.

(b) (7)(E)



(b) (7)(E)



IV. FINANCIAL PROVISIONS

A. Each party shall be responsible for its own costs in implementing this MOU.

B. Anti-Deficiency Act: Nothing contained herein shall be construed to violate the Anti-Deficiency Act, 31 U.S.C. § 1341, by obligating the BOP to any expenditure or obligation of funds in excess or in advance of appropriations.

V. GENERAL PROVISIONS

A. Period of Agreement/Termination:

1. This MOU shall become effective upon the date of final signatures of both parties, as designated below, and remain in effect for three years from the date of final signature.

2. This MOU may be terminated at any time by mutual written agreement; or by either party upon thirty (30) days advanced written notice to the other party, or immediately, with written notice to the other party,

upon violation of the terms and conditions of this MOU.

3. The provisions of this MOU which require performance after the termination of this MOU, e.g. third party disclosures, shall remain in force notwithstanding the termination of this MOU.

4. If any provisions of this MOU are determined to be invalid or unenforceable, the remaining provisions shall remain in force and unaffected to the fullest extent permitted by law and regulation.

5. Neither party shall be responsible for delays or failures in performance from acts beyond the reasonable control of such party, e.g., a natural or man-made disaster.

6. This Agreement shall remain in effect during the term in office of any succeeding leadership of either party, unless terminated or modified as provided herein.

B. **Modification Procedures:** All proposed modifications of this MOU shall be in writing and shall become effective only upon the written agreement of both parties.

C. **Dispute Resolution:** In the event of a dispute between the parties, the parties agree that they will use their best efforts to resolve that dispute in an informal fashion through consultation and communication, or other forms of non-binding alternative dispute resolution mutually acceptable to the parties.

D. **Liability/Indemnification:**

1. Each party shall be responsible for any liability arising from its own conduct and retain immunity and all defenses available to them pursuant to federal law. Neither party agrees to insure, defend, or indemnify the other party.

2. Each party shall cooperate with the other party in the investigation/resolution of administrative actions and/or litigation arising from conduct related to the responsibilities and procedures

addressed herein.

E. Contact persons. Each party shall provide to the other party, and update as necessary, the names, positions, telephone numbers and e-mail addresses for contact persons authorized to implement this MOU and coordinate additional operational details. At the time of signature, the parties have designated the following points of contact:

1. For technical/operational issues:

For BOP:

Bob Basile, Chief
Information Technology Security & Audit Compliance
Section
Trust Fund Branch
Federal Bureau of Prisons
500 First St, NW
Washington, DC 20534
Tel: (202) 514-2555 X7
E-mail: BBasile@bop.gov

For OIG:

Mike Reutemann, Wide Area Network Administrator
Office of Information Technology Management and Planning
Division
Office of the Inspector General
1425 New York Avenue, NW
Suite 13019
Washington, DC 20005
Tel: (202) 616-4556
E-Mail: Michael.J.Reutemann@usdoj.gov

2. For MOU administration/legal issues: For


BOP:

Dominique Raia, Senior Counsel
Office of General Counsel
Federal Bureau of Prisons
320 First St NW
Washington, DC 20534
Tel: (202) 353-8250

E-mail: draia@bop.gov

For OIG:

Gene E. Morrison, Special Agent in Charge
Immediate Office
Investigations Division
1425 New York Avenue, NW
Suite 7100
Washington, DC 20005
Tel: (202) 616-4760
E-Mail: Gene.E.Morrison@usdoj.gov
IN WITNESS WHEREOF, the undersigned, duly authorized
officers have subscribed their names on behalf of the
Federal Bureau of Prisons and the Office of the Inspector
General:

For the Federal Bureau of Prisons: 

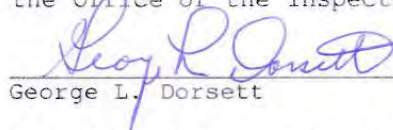


10/22/13

William F. Dalius
Assistant Director
Administration Division

Date

For the Office of the Inspector General:



10/29/13

George L. Dorsett

Date

Assistant Inspector General
Investigations Division

APPENDIX B

**Policy Concerning Electronic Recording of Statements
(Deputy Attorney General Memorandum, May 12, 2014)**

REFER TO ODAG

INSPECTOR GENERAL MANUAL
Volume III, Chapter 207
Management of Investigations
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was previously revised on September 23, 2009, and April 23, 2007, and originally issued on September 22, 1997. This chapter has been rewritten to reflect updates and changes in policies, laws, and guidelines.

*Changes issued in **XXXXXX**, appear in the following section:*

- 207.5B:** Revised to 1) increase the time frame requirements for completing cases—once criminal aspects have been completed—from 90 to 120 days, and 2) require agents to consult with a federal prosecutor at an early stage of each criminal investigation.
- 207.5E:** Adds guidance requiring all agents to conduct investigations in compliance with Rehabilitation Act principles and with all related OIG policies and guidance issued.
- 207.6B, C:** Rescinds paragraph the Priority Investigations Report requirement and combines the paragraphs as 207.6B.
- 207.7:** Revised to require that all documents placed in the case file folder must be uploaded to iManage contemporaneously with their addition to the case file.
- 207.7E:** Revises guidance on preserving investigative notes once an investigation has closed.
- 207.8:** Moves MOI format guidance to IGM III-210.5.
- 207.9:** Moves ROI format guidance to IGM III-210.6 and moves exhibit guidance to IGM III-210.10. Provides changes in Distribution procedures, including uploading to iManage.
- 207.9B(3):** Adds guidance on whether an ROI or investigative summary will be posted to the OIG public website.
- 207.10:** Moves AROI format guidance to IGM III-210.7 and moves exhibit guidance to IGM III-210.10. Provides changes in Distribution procedures, including uploading to iManage.
- 207.11A(4)** Revised to require field office SACs to discuss each case possibly falling under the category of “Sensitive or Unusual Cases” with the SAC, Operations Branch I or Operations Branch II, INV Headquarters, before designating it as a priority case.
- 207.11A(5):** Adds Deputy Attorney General Briefed Cases as a category of priority investigation.
- 207.11B:** Revises guidance on when investigative work agreements are necessary for priority investigations.

- 207.11D:** Rescinds guidance on bimonthly Priority Investigations Report due to cessation of report.
- 207.12B/B(1):** Revised to provide for changes in distribution procedures of interim ROIs, including uploading to iManage.
- 207.14:** Revised to provide “formal e-mail” as a means of requesting an AUX investigation and revises distribution procedures to include uploading to iManage.
- 207.15C:** Renames subsection D OIG/Field Office/Agent Responsibility
- 207.16A(8):** Adds guidance and an exception on the use of audio or audio-video recording of sworn statements for criminal and administrative cases.
- 207.16F:** Removes reference to priority investigations and rescinds requiring prosecutor’s approval of audio or video recording of sworn statements.
- 207.16G:** Revised to require compliance with DOJ Policy Concerning Electronic Recording of Custodial Statements.
- 207.16H:** Revised to require agents to provide copies of warning forms signed during an interview if requested by interviewees or their representatives.
- 207.18B:** Removes guidance on Investigation Extension Requests and re-letters subsections.
- 207.19:** Revises guidance on items that are not imported into iManage and provides for changes in distribution procedures to be issued by INV Headquarters. Adds guidance requiring agents to upload R-84 (final disposition reports) to iManage.
- 207.20A-D:** Moves PPR subsections A and B to IGM III-210, and re-letters subsections C and D as A and B.
- 207.20B:** Provides guidance on determining when a PRR should be posted to the OIG public website.
- 207.21A(2)(3):** Rescinds file folder maintenance for monitored referral investigations and requires uploading final reports to iManage.
- 207.23G:** Adds guidance on (b) (7)(E) recordkeeping.
- Appendices:** A – O removed from chapter and made available on SharePoint
- Appendix P:** Memorandum of understanding between the OIG and BOP concerning OIG use of (b) (7)(E) moved to Appendix A.
- Appendix B:** Adds DAG Policy Concerning Electronic Recording of Statements to Appendix B.

Changes issued in FY17-POL-06, March 14, 2017, appear in the following section:

207.6B(1): Requires a standardized procedure for documenting case reviews.

Changes issued in FY17-POL-03, February 2, 2017, appear in the following section:

207.4D: Standardizes the requirement to notify the FBI of any opening of a criminal case of concurrent jurisdiction.

Changes issued in FY17-POL-07, April 12, 2017, appear in the following section:

207.25: Adds guidance requiring the notification of investigations involving certain ethics violations to the Office of Government Ethics.

Changes issued in FY15-POL-02, July 28, 2015, appear in the following section:

207.24K In coordination with IGM III-205.12, establishes procedures for processing non-DOJ PREA allegations.

Changes issued by DAIG, INV, e-mail, effective January 20, 2015, appear in the following section:

Appendix O: Revises the ROI review process.

Changes issued by e-mail in FY14-POL-03, July 9, 2014, appear in the following section:

207.24: Incorporates existing guidance and training, in conformance with the Prison Rape Elimination Act, into policy concerning the processing and investigation of allegations of sexual abuse in confinement settings.

Changes issued by Deputy Attorney General Memorandum, May 12, 2014, appear in the following section:

207.16G

and

Appendix Q: Policy establishes a presumption that statements of persons in custody of DOJ components will be recorded and sets forth the circumstances.

Changes issued in FY14-POL-02, April 30, 2014, appear in the following section:

Appendix N: Revises OIG Form III-207/9 (Agreement of Attorney to Maintain Confidentiality and Nondisclosure of Information).

Changes issued by e-mail, January 12, 2012, appear in the following section:

207.19D Clarifies the requirement issued in FY11-POL-08 to upload documents into iManage and provides file name examples for uploaded documents.

Changes issued in FY12-POL-01, November 2, 2011, appear in the following sections:

207.7E Adds guidance regarding disposition of electronic communications.

- 207.8C(3)** Revises guidance regarding MOI content, aligning with FY11-POL-06 policy change, eliminating an MOI requirement for an affidavit or recorded interview except for unusual circumstances or other relevant information.
- 207.8C(9)** Adds guidance regarding reporting electronic communications in the MOI.
- 207.8E** Revises MOI exceptions, aligning with FY11-POL-06 policy change.

Change issued in FY11-POL-08, March 9, 2011, appears in the following section:

- 207.19D** Expands the required documents to be uploaded into iManage and excepts classified, grand jury, and voluminous collected documents.

Changes issued in FY11-POL-06, February 9, 2011, appear in the following sections:

- 207.8C(3)** Revises MOI requirement for an affidavit or recorded interview except to report unusual circumstances.
- 207.8E** Specifies circumstances when an MOI is not required.
- 207.17** Deleted requirement for transcript page and paragraph number references for pertinent information in MOI.

Changes issued in FY11-POL-05, February 4, 2011, appear in the following sections:

- 207.5A(4)** Specifies use of the IDMS Case Status Screen (formerly “scratch pad”) in documenting discoverable information, including content, format, and examples.
- 207.5B(3)** Specifies that explanations of lack of case activity should not be in the case file, IDMS Case Status Screen, or an MOI.

Changes issued in FY10-POL-02, July 28, 2010, appear in the following sections:

- 207.14:** In paragraphs A(3), B, D, and E, changes add clarification that the controlling office will be in possession of the original documents at the completion of an AUX investigation.

Changes, additions, and deletions in guidance issued September 23, 2009, appear in the following sections:

- 207.4C:** Adds a new first sentence describing IDMS and introduces the new IDMS acronym (changed throughout Chapter guidance).
- 207.4C(1):** Adds a third opening status code, OPIN.

- 207.5C(2)a:** Deletes the second sentence, regarding 90-day completion of investigations.
- 207.6A:** Replaces the SACS Report with the Field Office Productivity Chart, generated by INV Headquarters from IDMS data.
- 207.6B:** Replaces the Monthly Report of Priority Investigations with a bimonthly report (every 2 months).
- 207.6C(2):** Deletes the last sentence, removing the requirement for SAC review every 60 days.
- 206.6C(3):** Revises the sentence regarding data and report review media in priority and over-age investigations.
- 207.7C(2):** Requires formal case review at intervals of at least every 60 days and permits optional use of case record (Appendix B) or guideline materials (Appendix G).
- 207.7D(9):** Adds compelled statements to the list of items required to be marked on the outside of the case file.
- 207.8C(8):** Adds guidance regarding PII content in MOIs.
- 207.11C(2):** Adds guidance regarding the report review process.
- 207.11D:** Changes the report reference to specify the Priority Investigations Report and bimonthly (every 2 months) preparation.
- 207.11D(2):** Changes the Priority Investigations Report frequency to bimonthly (every 2 months).
- 207.16F:** Adds new guidance regarding required tape recording and recommended tape recording of subjects and witnesses.
- 207.16F(12):** Provides guidance regarding handling of original tape recordings of subjects and witnesses.
- 207.17:** Adds guidance regarding annotating pertinent transcript page numbers in MOIs.
- 207.19C(2):** Adds guidance regarding ASAC/SAC responsibility for completed reports.
- 207.19D:** Inserts a new paragraph D (guidance requiring document management of MOIs in iManage) and changes the following paragraph numbers to 207.19E-G.
- 207.22:** Adds a definition and guidance for conducting initiatives.
- 207.23:** Adds policy regarding the use of (b) (7)(E) database searches in BOP investigations.
- Appendix B:** Updates OIG Form III-207/6.

Appendix G: Adds ROI tracking compliance to the supervisor's checklist.

Appendix J: Changes the reporting time period for the Priority Investigations Report to bimonthly (every 2 months).

Appendix N: Provides the current OIG Form III-207/9 (Agreement to Maintain Confidentiality and Nondisclosure of Information), revised December 11, 2007.

Appendix O: Adds an outline of the Report Review Process.

Appendix P: Adds the memorandum of understanding between the OIG and BOP concerning OIG use of (b) (7)(E).

- 210.1 Policy. This chapter establishes policies and procedures for high quality writing in all investigative documents produced by the Office of the Inspector General (OIG) Investigations Division (INV).
- 210.2 Reference. This chapter is issued under the authority of the Inspector General and the Assistant Inspector General for Investigations to establish and disseminate quality standards for all documents produced by the INV.
- 210.3 Scope. The provisions of this chapter apply to all employees of the INV.
- 210.4 Report Writing Guidelines That Apply to All Investigative Documents. This section summarizes OIG report writing policy that applies to all investigative documents. Additional writing instructions can be found in the "OIG Style Manual" on M&P's SharePoint page and in the INV training manuals entitled "Writing, Reviewing, Investigating" and "Writing Samples."
- A. Application. These report writing rules apply to the following documents and reports:
- (1) Memorandum of Investigation (MOI).
 - (2) Report of Investigation (ROI).
 - (3) Abbreviated Report of Investigation (AROI).
 - (4) Procedural Reform Recommendation (PRR).
- B. Content Standards. OIG investigative documents should be objective, focused, and logically constructed so that any reader unfamiliar with the investigation will understand the issues and the investigative results.
- (1) Accuracy in collecting and reporting facts is essential to sustain criminal, civil, or administrative actions. No opinions, footnotes, or agent's notes will appear in any MOI, ROI, or AROI. Investigative documents must distinguish facts from hearsay, conclusions, or inferences and must use the proper words to express facts. Hearsay information must be reported as such.
 - (2) Do not report ambiguous terms used by persons interviewed, such as "occasional" or "infrequently," without defining as precisely as possible what the individual meant by those terms. When referring to periods of time such as "last week," or "last month," indicate by actual dates (for example, "the week beginning May 5, 2018," or "July 2018"). Questions raised by an interview must not be left unanswered or open to misinterpretation.

- (3) Agents must normally identify sources of information. For exceptions, see instructions regarding employee complainant confidentiality rules (Inspector General Manual (IGM), Volume III, Chapter 205) (IGM III-205) and rules regarding confidential sources (IGM III-240).
 - (4) If information is obtained by means other than a personal interview, indicate the method (that is, by letter or by telephone).
 - (5) Indicate if the interviewee provided an affidavit or recorded sworn statement.
 - (6) Briefly and accurately state the relevant information provided by the person interviewed. Identify any records a witness furnished. Avoid reporting extraneous information.
 - (7) Do not quote an entire written statement verbatim in an MOI or ROI. A written statement will normally be an attachment to an exhibit item. Provide an accurate, concise summary of the relevant parts of statement information.
 - (8) Do not report information provided by a witness solely for the purpose of identifying other possible areas of investigation.
 - (9) Other than the use of a person's name, the use of personally identifiable information (PII) in AROIs and ROIs is prohibited. PII is defined as information that uniquely identifies an individual and may include, but is not necessarily limited to, full Social Security numbers, taxpayer identification numbers, driver's license numbers, license plate numbers, credit card numbers, current and previous home addresses, current and previous home telephone numbers, birthdates, and family and medical information.
- C. **Format and Style Standards.** Reports should be prepared in accordance with the current OIG Style Manual and the appropriate Format and Style Standards Guides referenced in this chapter as appropriate.
- 210.5 **Memorandum of Investigation Guidelines.** Report a particular investigative activity or facet of an investigation using OIG Form III-210/4 (Memorandum of Investigation) (MOI). Blank MOI forms are available at *SharePoint Forms: IG Manual*.
- A. **Quality Standards.** MOIs must be concise but comprehensive and must be logically organized. Use subcaptions to help organize MOIs of two or more pages. Further instructions regarding MOI content are contained in the *MOI Format and Style Standards Guide* (OIG Guide III-210/4) available on SharePoint.
 - B. **Personally Identifiable Information.** Refrain from using PII in an MOI, such as dates of birth, addresses, and Social Security numbers, if the information is not directly pertinent to an investigation. If created by INV, MOIs and other documents

containing PII material will not be distributed outside of DOJ OIG unless the material is specifically required by a prosecutor, an administrative law judge, or the component. If the documents are obtained from other agencies, the documents containing PII will only be distributed after consent is given from the originating agency. PII may be contained in the online Investigations Data Management System, investigative notes, or other documents that remain in the case file.

- C. Separate Activities. Agents will report by separate MOI each investigative activity or interview. If, however, witnesses (not subjects) are interviewed together, one MOI may be prepared to record the joint interview.
- D. MOI Preparation Timeframes. Agents will prepare MOIs by the end of the fifth workday after the investigative activity or as soon as is reasonably possible after the fifth workday as agreed upon by the SAC or ASAC. Adherence to this policy will help assure that pertinent information is recorded contemporaneously with the investigative activity and while still fresh in the agent's memory.
- E. Review and Approval. The ASAC or SAC will review each MOI for accuracy, completeness, and clarity.
- F. MOI Requirement Exceptions. Agents are not required to prepare an MOI in the following circumstances:
 - (1) when reporting investigative activities or interviews conducted jointly with another investigative agency and that agency is preparing the official record of the activity. Preparing two separate records of the same event must be avoided, where possible. The agencies should agree ahead of time to record the interview or activity in one document. For example, rather than each agency preparing a separate and possibly conflicting written record, the OIG and the FBI, working jointly, agree to record the investigative activity in an FBI 302. In this case, an MOI should not be prepared.
 - (2) when self-authenticating documents or evidence are obtained, a separate MOI is not required to introduce or summarize the document. Self-authentication implies the document requires no further explanation, that its relevance to the investigation is clear, and that the document describes when the activity took place and who was present. Examples of self-authenticating documents are a judgment and commitment order, a sworn affidavit, the transcript from a recorded interview, and a DEA-6 or FBI-302 reporting an event not conducted jointly with the OIG.

210.6 Report of Investigation Guidelines. The ROI reports the summarized results of an OIG investigation.

- A. **Concept and General Format.** The ROI will be clear, concise, and specific so as to guide the reader logically through the allegations, the scope of the investigation, significant interviews, and the investigative findings.

The ROI will introduce witnesses and report events and investigative results in a logical sequence. The ROI will be a narrative of significant facts and relevant information that concisely and precisely tells the reader what was determined by the OIG's investigation, supported by and consistent with the investigative activity recorded in MOIs.

An ROI is officially designated as form III-210/1, excluding the list of exhibits and the supporting exhibits. Once finalized, an ROI portfolio should be created. An ROI portfolio consists of the following:

- (1) OIG Form III-210/3 (Report of Investigation Cover Sheet) (*SharePoint Forms: IG Manual*). Completion of this form is self-explanatory.
- (2) OIG Form III-210/1 (Report of Investigation) (*SharePoint Forms: IG Manual*).
- (3) Exhibits that support the ROI, including copies of MOIs, affidavits, and other evidence. Refer to Appendix D of the *ROI Format and Style Standards Guide* (OIG Guide III-210/1) available on SharePoint for further information about exhibits.

- B. **Content Standards.** Agents report OIG investigations using OIG Form III-210/1. The ROI is to be written in short and simple sentences and paragraphs, without sacrificing clarity, completeness, and accuracy. It should be no longer than necessary to communicate the relevant investigative findings properly.

- C. **ROI Format and Style Standards.** Agents must prepare ROIs in conformance with the current *ROI Format and Style Standards Guide* (OIG Guide III-210/1) issued by headquarters as posted in SharePoint.

210.7 **Abbreviated Report of Investigation Guidelines.** The Abbreviated Report of Investigation (AROI) is an optional alternative writing format for use when an investigation is being closed and can be reported in a brief synopsis. The AROI is not a chronological accounting of the investigation but, instead, must summarize the allegations and investigative findings in a few brief paragraphs. Agents must prepare AROIs in conformance with the current *AROI Format and Style Standards Guide* (OIG Guide III-210/2) issued by headquarters as posted in SharePoint.

210.8 **Procedural Reform Recommendation Guidelines.** Procedural Reform Recommendations (PRR) are important recommendations submitted to agency managers and, as such, require careful writing. A poorly written document may be difficult to understand and may discourage officials from reading the document and can prevent them from giving serious

attention to the OIG's recommendations. Agents must prepare PRRs in conformance with the current *PRR Format and Style Standards Guide* (OIG Guide III-210/3) issued by headquarters as posted in SharePoint.

- A. **Purpose.** The PRR brings program vulnerabilities discovered during an OIG investigation to the attention of component management, who can then correct the vulnerabilities. Reliance only on criminal prosecution or disciplinary action without correcting program weaknesses invites fraudulent practices to continue. The PRR enables INV to be proactive as well as reactive.
- B. **Content.** The PRR will concisely identify and analyze the systemic problem uncovered during the investigation. The PRR will be fully researched to identify existing DOJ component policy or procedures that relate to the problem, and a copy of the policy must be included with the PRR. The PRR will also recommend corrective action that gets at the root cause of the problem. Refer to IGM III-210 for PRR style and formatting guidelines.

210.9 **Supervisory Review of Investigative Documents.** The SAC and the ASAC must view the investigative process, including report writing, as a collaborative process — that is, agents and supervisors work together to produce the most effective results.

SACs and ASACs will develop a consistent review style that keeps the two major objectives of the review process in mind:

- A. **Objective One: Produce Quality Reports.** SACs and ASACs evaluate the report to ensure that it is the best product possible under investigative constraints. They check that data are accurate and meaningful and that the conclusions and recommendations are logical. The report must have solid investigative substance, and this substance must be presented logically. Supervisors ensure that writing techniques for focus and flow are used to clarify and emphasize the main points and further a smooth, logical flow of ideas.
- B. **Objective Two: Long-Term Writing Improvement.** SACs and ASACs foster professional development of their staffs by reinforcing the principles of good writing. They must insist that these principles are consistently applied and will refer to these principles when discussing report writing with staff members. These discussions can be with an individual agent and related to a specific report or in broader discussions in a group setting. This on-the-job training reinforces good writing principles for the writer and enables the writer to see definite strategies for improving his or her writing.

210.10 **Exhibits.** Exhibits permit the reader to examine complete copies of MOIs, sworn statements, financial data, or other records that are essential to comprehend the investigative findings fully. Exhibits to an ROI or AROI are essential to a reader's full comprehension of the investigative findings. All relevant exhibits that support the results of

investigation summarized in the synopsis will be prepared and attached in accordance with guidance provided in Appendix D of the *ROI Format and Style Standards Guide* (OIG Guide III-210/1).

INSPECTOR GENERAL MANUAL
Volume III, Chapter 210
Report Writing Procedures
Revisions

This chapter was previously revised on April 22, 2009, and originally issued on April 23, 2007. This chapter was rewritten to reflect updates and changes in policies, laws, and guidelines.

Changes issued in this partial revision, dated XXXX, appear in the following sections:

- 210.4C/210.6C:** Moves guidance on ROI format and style standards to a separate guidance document that will be made available on SharePoint.
- 210.5C:** Moves guidance on MOI format and style standards to a separate guidance document that will be made available on SharePoint.
- 210.5D:** Adds guidance on MOI preparation timeframes.
- 210.5E,F:** Adds guidance from III-207 pertaining to MOI Review and Approval and MOI Exceptions.
- 210.6A:** Adds clarifying language to ROI definition.
- 210.6A(3):** Moves guidance on Exhibits to Appendix D of the *ROI Format and Style Standards Guide* available on SharePoint.
- 210.7A-C:** Moves guidance on AROI format and style standards to a separate guidance document that will be made available on SharePoint.
- 210.8:** Adds definition of PRRs, Purpose, and Content. Moved from IGM III-207. Moves guidance on PRR format and style standards to a separate guidance document that will be made available on SharePoint.
- 210.10A-G** Removes subsections A-G from IGM chapter and makes Exhibits guidance available in Appendix D of the *ROI Format and Style Standards Guide*.
- Appendices** Removes appendices A – E from IGM chapter and makes forms available on SharePoint Forms: IG Manual.

Changes, additions, and deletions in guidance dated April 22, 2009, appear in the following sections:

- 210.4B(9):** Adds guidance limiting and defining PII used in AROIs and ROIs.
- 210.4C(4) and 210.4C(4)a:** Changes guidance regarding acronym introduction and use.
- 210.5 and 210.5B:** Adds information regarding MOI creation and adds guidance limiting PII in MOIs and limiting distribution of MOIs that contain PII.
- 210.6C(1)a, b:** Changes the guidance regarding ROI subject identification, limiting the information to the full name and partial Social Security number.
- Appendix B:** Changes the report cover sheet, adding the marking “SENSITIVE BUT UNCLASSIFIED.”

From: [Warren, James W \(OIG\)](#)
To: [IGNITE \(INV\)](#)
Cc: [Blier, William M.\(OIG\)](#)
Subject: (b) (7)(E)
Date: Tuesday, September 04, 2012 10:17:06 AM

INV Staff,

Often, OIG agents work with other components or agencies (such as the FBI) in BOP prison cases. Frequently, those cases involve (b) (7)(E). We, the OIG, are always diligent in obtaining the appropriate approvals from the Office of Enforcement Operations (OEO) and the BOP. However, there are instances where agents from other agencies – generally due to lack of awareness of OEO approval requirements plan operations without obtaining the proper approvals. Our agents have worked with those agents to educate them and to ensure that the proper approvals are obtained.

It is important that we continue to ensure that proper approvals are obtained in these cases. If you become aware of an agent from another agency planning to proceed with an operation without obtaining required OEO approval either intentionally or due to lack of awareness of the requirement, please contact me or ASAC John Regan. We work closely with OEO on these issues. Because of reported incidents, OEO is enhancing its education efforts for the other components and agencies.

(b) (7)(E) please be sure to include in a separate section (if not already explicitly recorded in the narrative of the request) if there are other agencies participating in the investigation and if so what their roles are. If there are no other agencies participating in the investigation, please make an affirmative statement as such.

As a reminder, if circumstances change from what was approved (b) (7)(E), please let me or ASAC Regan know so that we can advise OEO and obtain additional approval if necessary.

Thanks,
Chip

James (Chip) Warren
Special Agent in Charge
Investigative Support Branch
Department of Justice
Office of the Inspector General
Tel: (202) 616-4729

SENSITIVE BUT UNCLASSIFIED

223.1 **Policy.** This chapter establishes policy and procedures for the use and protection of

(b) (7)(E)

In order to facilitate the conduct of investigations and resolution of allegations, the Office of the Inspector General (OIG) may use the information and assistance (b) (7)(E)

Investigative activities using such persons shall:

- A. take all reasonable steps to ensure the safety and well-being of individuals who provide information and assistance to the OIG and
- B. adhere to applicable laws and regulations governing the activities of persons in custody and protected witnesses.

Certain policies and procedures set forth in this chapter must be carried out in conjunction with related policies in the Inspector General Manual (IGM), Volume III, Chapters 240 (III-240), "Informants"; III-250, "Undercover Operations Guidelines"; and III-260, "Electronic Surveillance."

223.2 **Reference.** This chapter is issued under the Inspector General Act of 1978, as amended; Attorney General Guidelines for the Use of Confidential Informants, dated May 30, 2002; and Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority, dated December 8, 2003.

223.3 **Scope.** The provisions of this chapter apply to all employees of the OIG Investigations Division (INV).

223.4 **Definitions.**

- A. **Persons in Custody.** For the purposes of this chapter, persons in custody include persons legally in the custody of the U.S. Marshals Service (USMS), BOP, or U.S. Parole Commission. Persons in custody may be sentenced offenders serving a term in the custody of the Attorney General or persons who are under custodial supervision awaiting trial or sentencing. Persons who are under supervision of a U.S. district court following suspension of the imposition or execution of sentence are considered persons in custody for the purposes of this chapter, and communication from the OIG regarding the use of such a person should be directed to the chief U.S. probation officer for the judicial district where the sentence was suspended.

B.

(b) (7)(E)

(b) (7)(E)



D. Principal. (b) (7)(E)



E. Authorized Dependent. (b) (7)(E)



F. Witness Control Number. (b) (7)(E)



G. Sponsoring Attorney. (b) (7)(E)



H. Danger or Threat Area. (b) (7)(E)



223.5 (b) (7)(E)



A. Required Consultation.



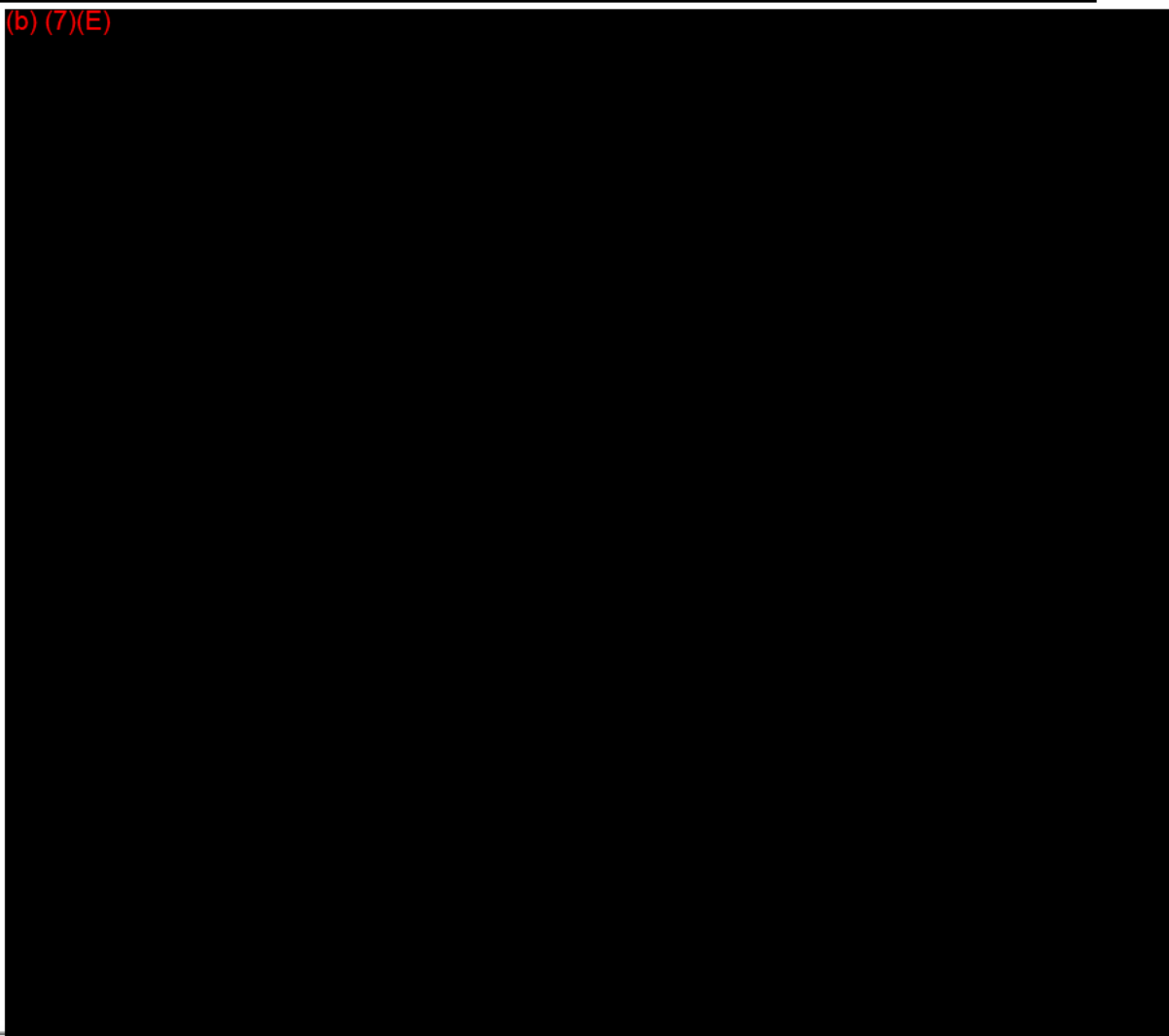
(b) (7)(E)

A large black rectangular redaction box covering the top right portion of the page.

(b) (7)(E)

A large black rectangular redaction box covering the middle portion of the page.

B. (b) (7)(E)

A very large black rectangular redaction box covering the bottom two-thirds of the page.

(b) (7)(E)

C. Authorization. (b) (7)(E)

D. Documentation. (b) (7)(E)

E. Additional Concerns. (b) (7)(E)

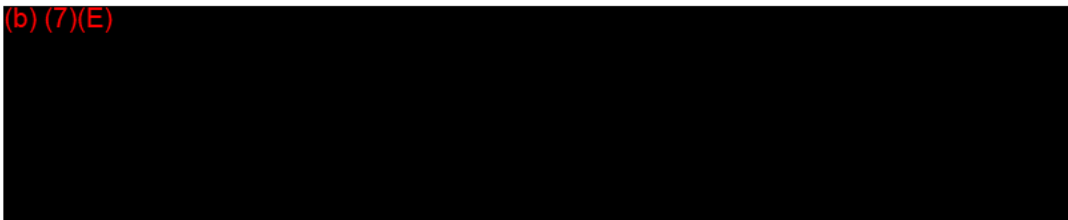
F. OIG Agents and BOP Regulations. Whenever an OIG agent contacts a person in BOP custody, (b) (7)(E)

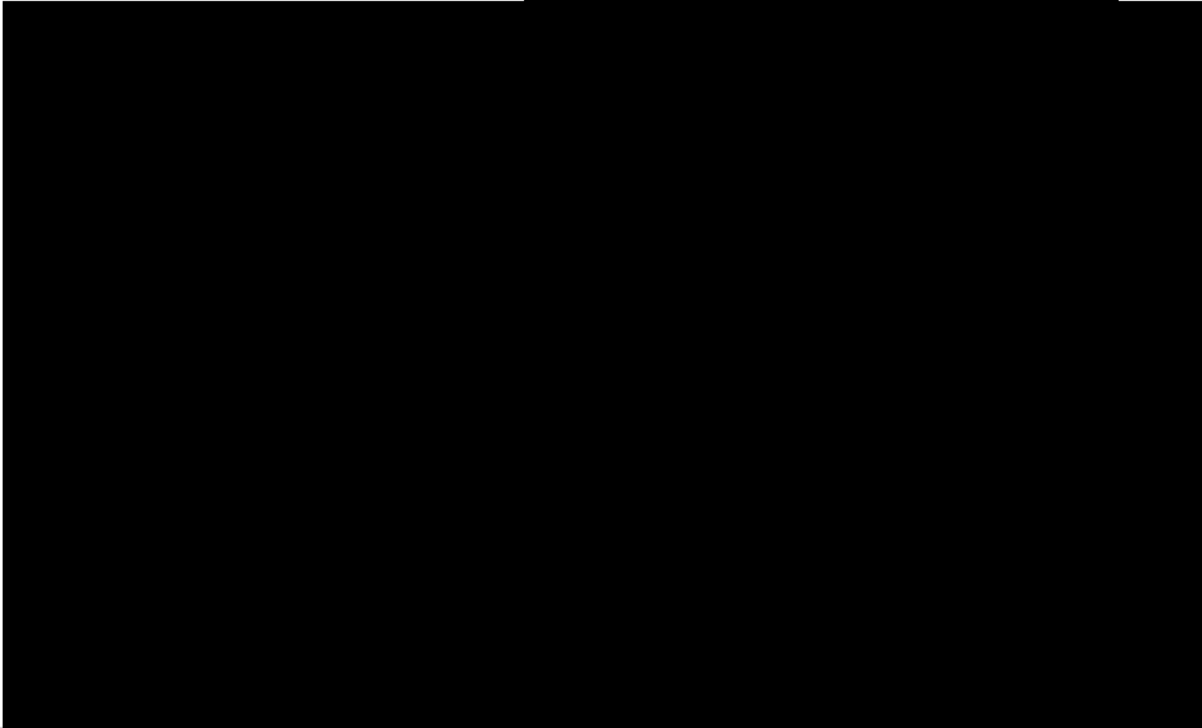
the agent must abide by BOP rules and regulations, including the following:

- (1) The BOP forbids its employees from providing anything (even items of nominal value) to prisoners that is not available to all prisoners on the same

basis. For example, a BOP employee supervising an inmate work crew may not provide cigarettes, soft drinks, snacks, or anything else the employee might purchase for the inmate crew, even as a reward for outstanding effort. This policy is strictly enforced, and violations often lead to disciplinary action against BOP employees. OIG employees contacting a BOP inmate for any reason must be aware of this policy and ensure that any tobacco products, food items, or drinks provided to prisoners come only from official BOP sources.

- (2) If an agent who is interviewing an inmate expects that the session will go past the next scheduled meal time, the agent should either obtain the voluntary agreement of the prisoner to waive the meal or arrange for the prisoner to receive a meal. Unless the inmate is in the Special Housing Unit, the inmate will normally have to go to the institution dining hall to receive the meal. The agent may be able to arrange for the inmate meal to be served in the interview room, but this service must be arranged in advance with the institution's warden or his or her designee.

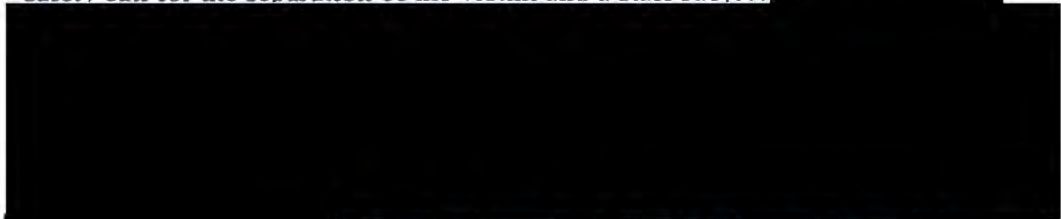
- (3) (b) (7)(E)
- 

- G. Exception to Departmental Approval. (b) (7)(E)
- 

(b) (7)(E)



H. Inmate Victims of Sexual Abuse. Prison Rape Elimination Act protocols for victim safety call for the separation of the victim and a staff subject. (b) (7)(E)



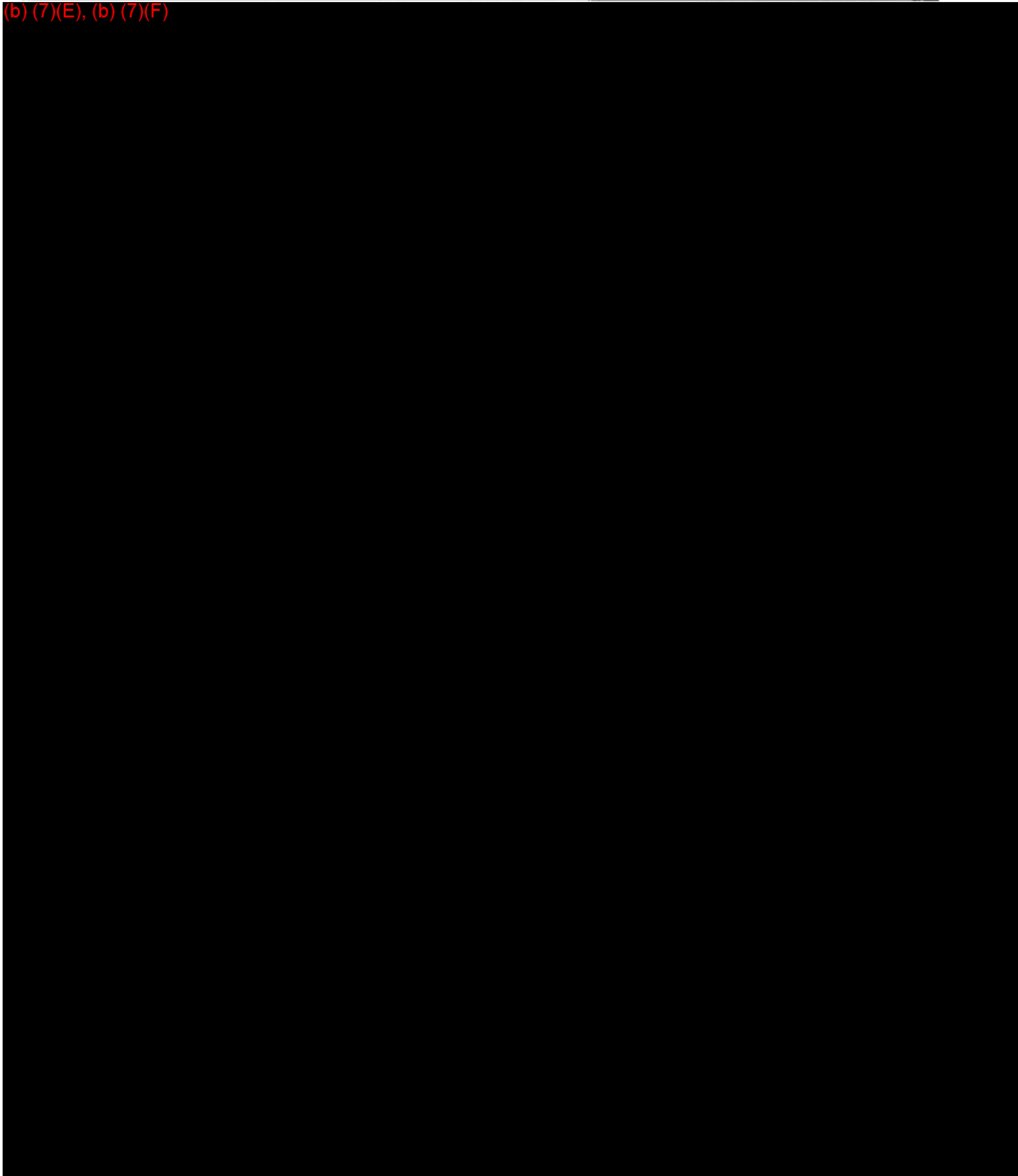
(See also Appendix C for definitions of sexual abuse and harassment terms in the Prison Rape Elimination Act.)

223.6 Special Precautions Involving (b) (7)(E)

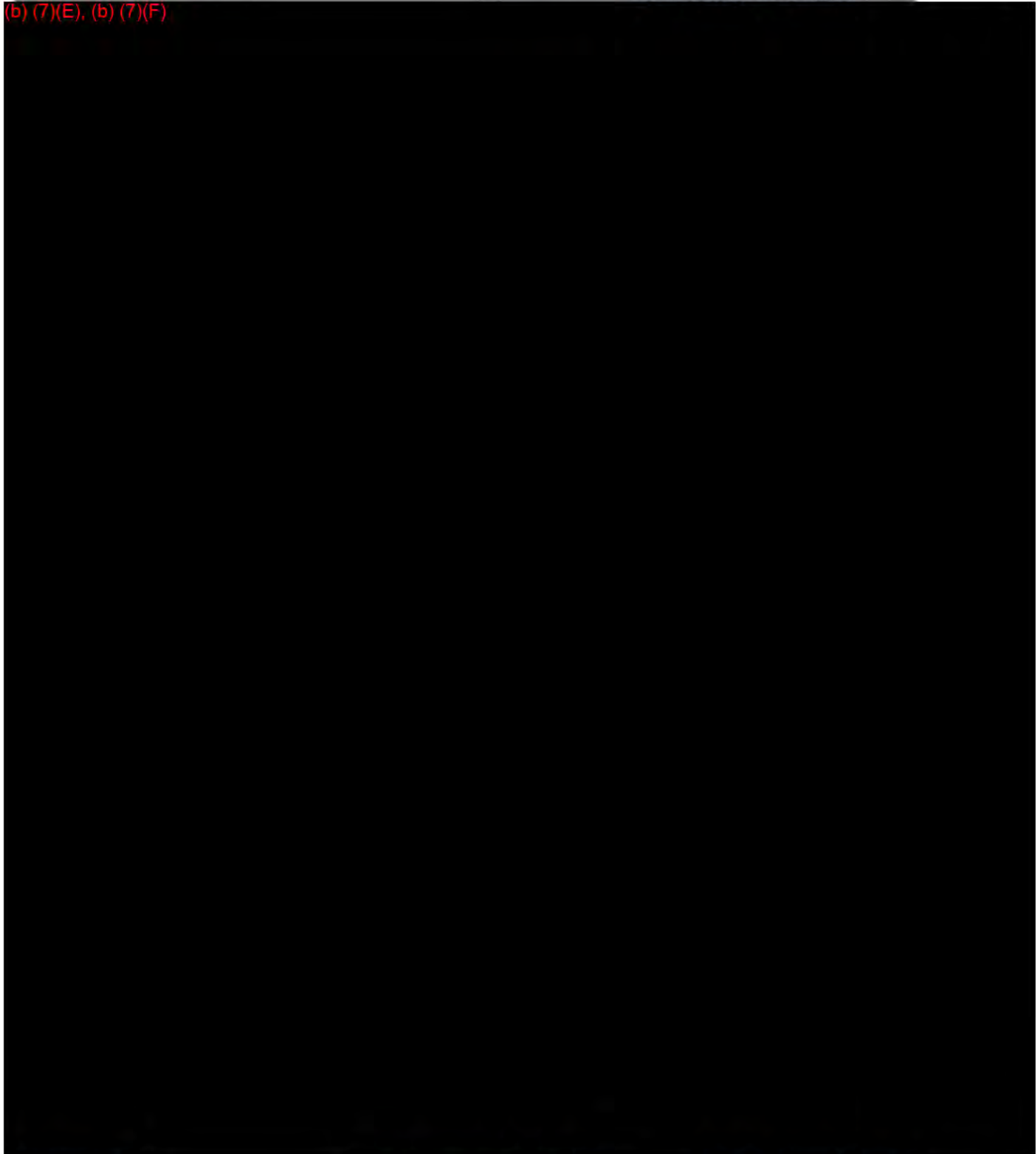


(b) (7)(E)

(b) (7)(E), (b) (7)(F)



(b) (7)(E), (b) (7)(F)

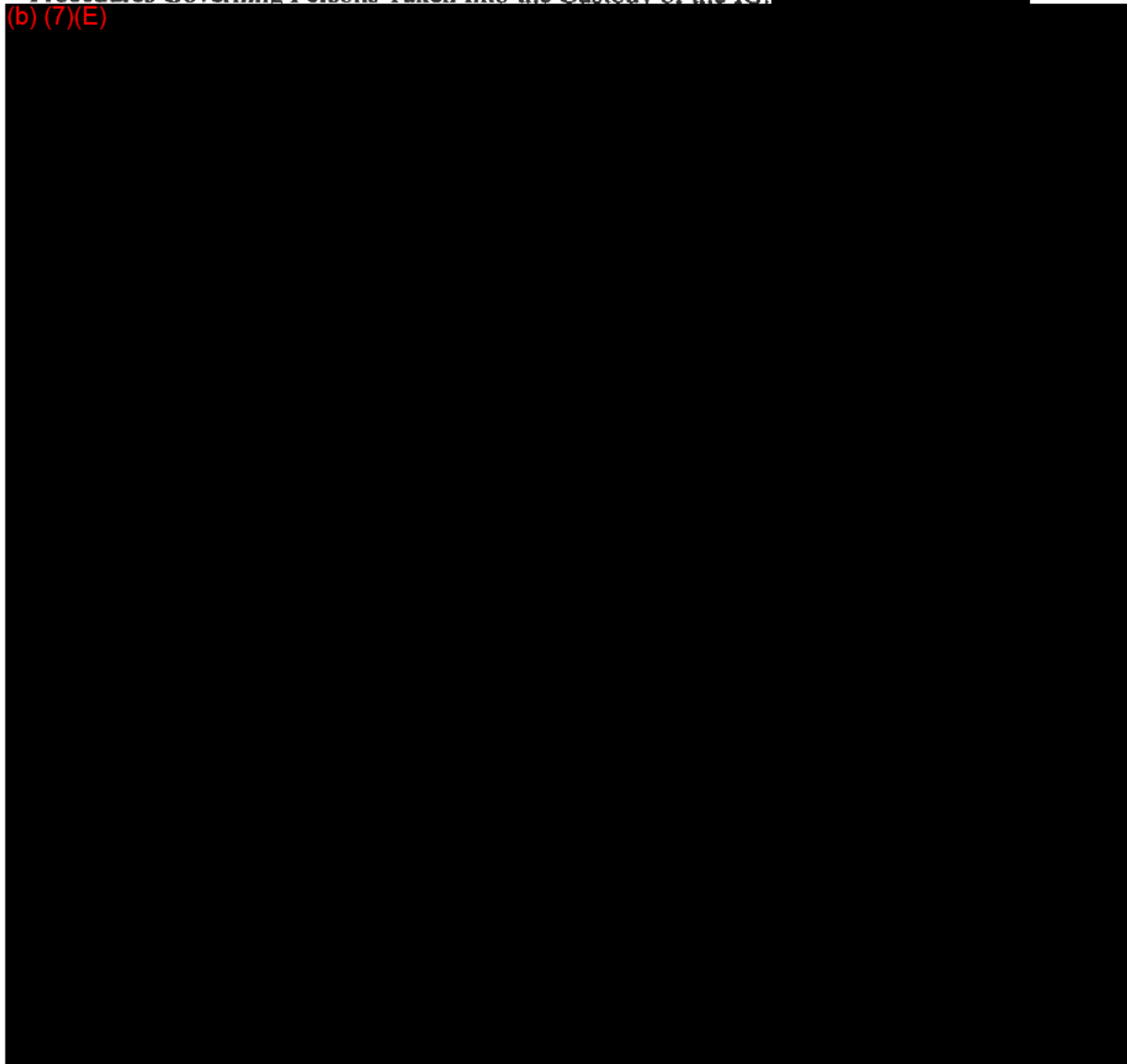


(b) (7)(E), (b) (7)(F)



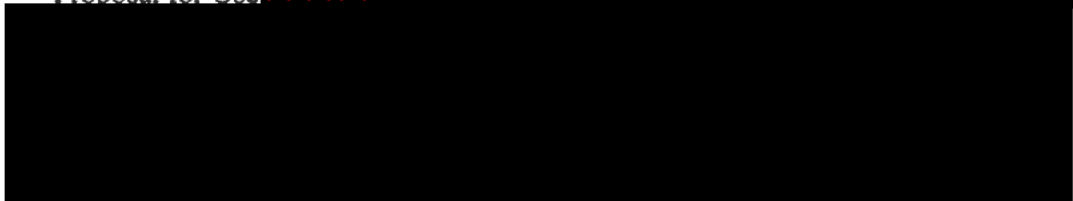
223.10 Procedures Governing Persons Taken Into the Custody of the IG.

(b) (7)(E)



223.11

A. Proposal for Use (b) (7)(E)



(b) (7)(E)



B. Conditions of Use (b) (7)(E)



C. Agreement (b) (7)(E)



223.12

(b) (7)(E)



223.13

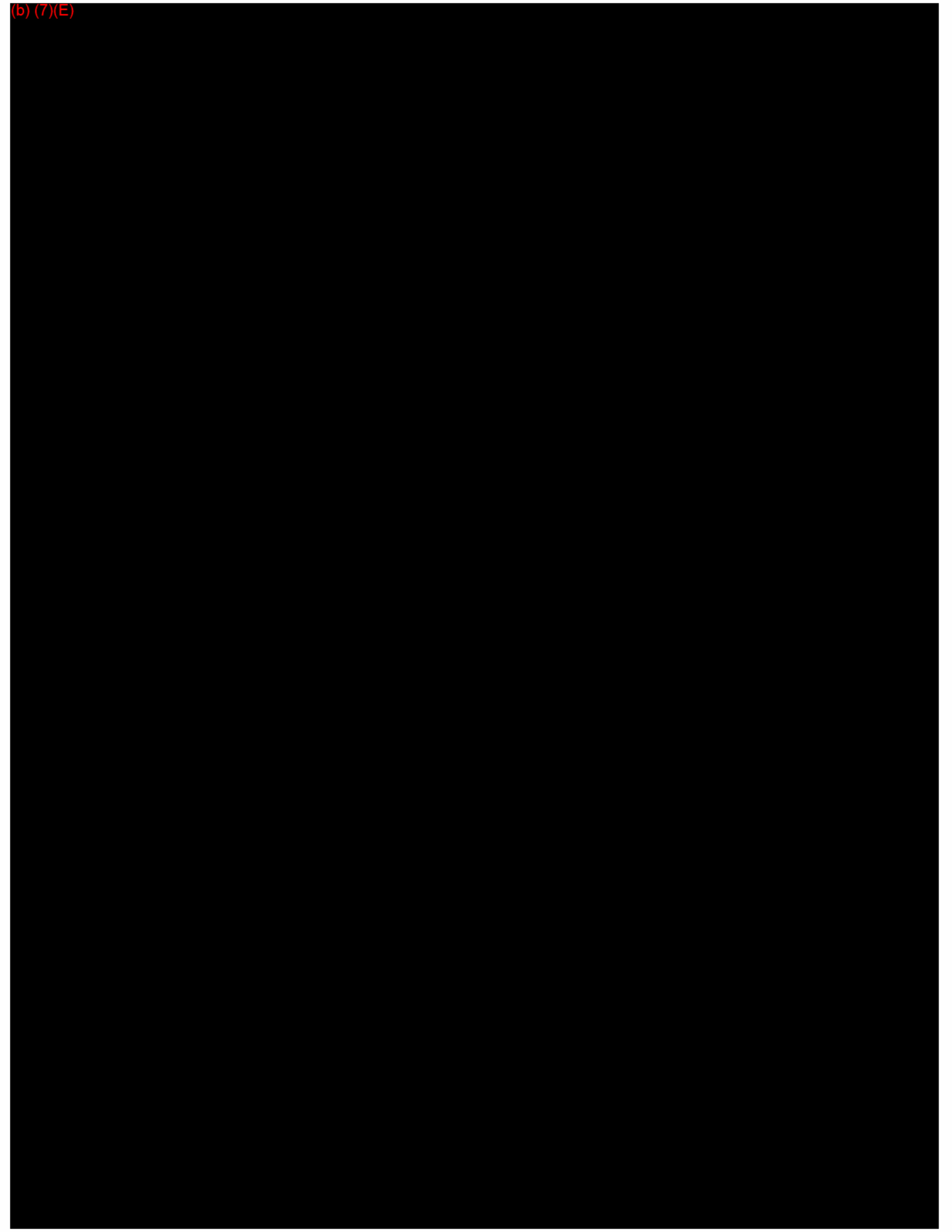
(b) (7)(E)



APPENDIX A

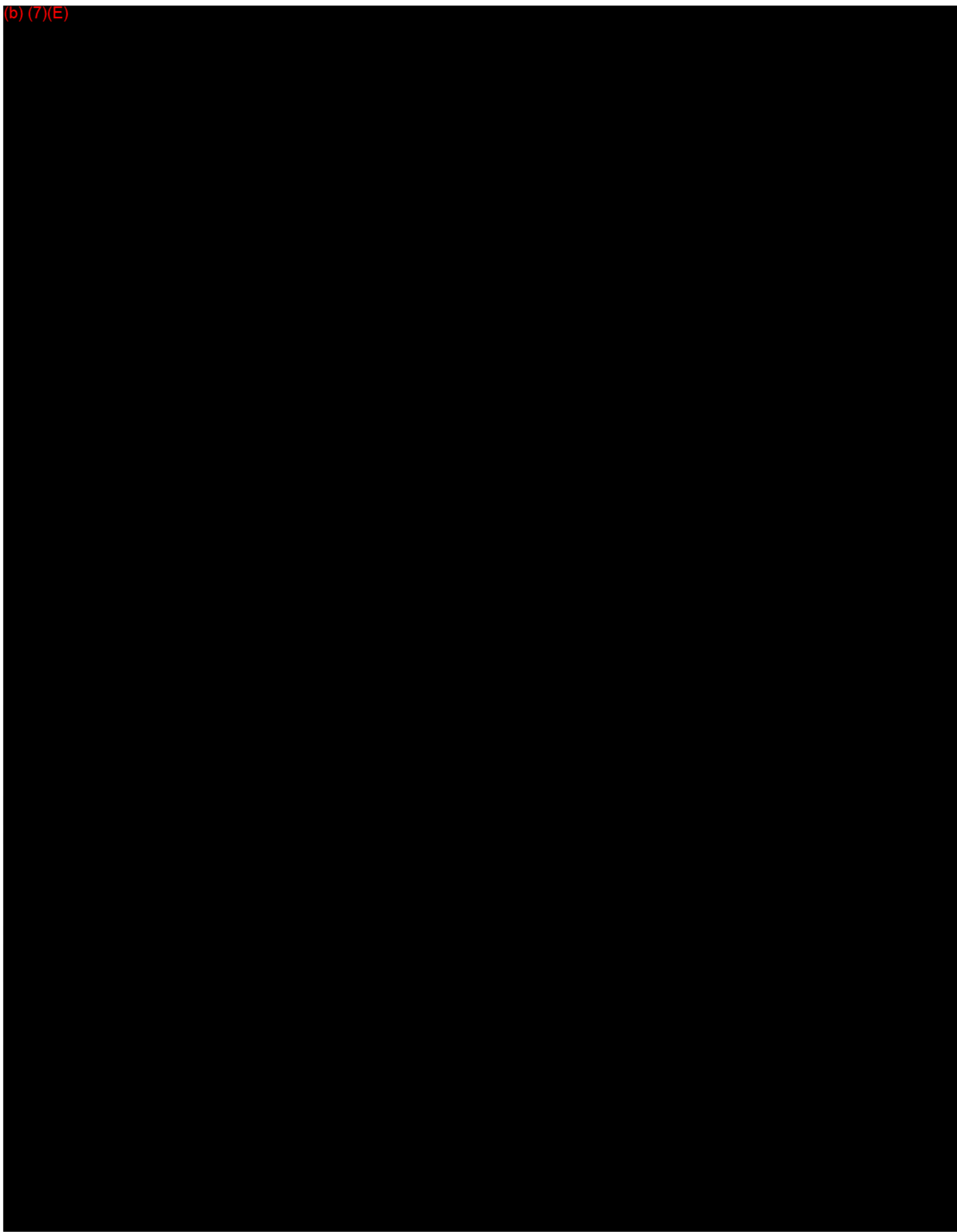
(b) (7)(E)





(b) (7)(E)





(b) (7)(E)



APPENDIX C

Definitions of Terms in the Prison Rape Elimination Act

DEFINITIONS OF TERMS IN THE PRISON RAPE ELIMINATION ACT

The definition of *sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer* includes any of the following acts, with or without consent of the inmate, detainee, or resident:

- (1) contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) contact between the mouth and the penis, vulva, or anus;
- (3) contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (4) penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (5) any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (6) any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1)-(5);
- (7) any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of an inmate, detainee, or resident, and
- (8) voyeurism by a staff member, contractor, or volunteer.

Voyeurism by a staff member, contractor, or volunteer means an invasion of privacy of an inmate, detainee, or resident by staff for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring an inmate to expose his or her buttocks, genitals, or breasts; or taking images of all or part of an inmate's naked body or of an inmate performing bodily functions.

Sexual harassment in a confinement setting includes:

- (1) repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- (2) repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 223
Use of Persons in Custody and Protected Witnesses
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was previously revised on April 23, 2007, and originally issued on October 15, 1992. This chapter was rewritten to reflect updates and changes in policies, laws, and guidelines.

This chapter revision includes an inserted revised policy, approved by the Inspector General or his Designee, issued July 9, 2014:

This policy addition is in conformance with the Prison Rape Elimination Act (PREA), Public Law 108-79, which was passed unanimously by Congress in 2003, and AG Order No. RIN 1105-AB34, as codified in the Code of Federal Regulations (C.F.R.), Title 28, Part 115, on May 16, 2012. (See also www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf.)

223.5H: Adds guidance concerning processing and investigation of allegations of sexual abuse in confinement settings (Policy Memorandum FY 14-POL-03).

Appendix C: Adds Definitions of Terms in the Prison Rape Elimination Act (Policy Memorandum FY 14-POL-03).

Changes, additions, and deletions in guidance issued August 26, 2009, appear in the following sections:

223.5A(1): Adds cross-reference to guidance regarding an exception (b) (7)(E)

223.5A(2): Adds guidance regarding required consultation (b) (7)(E)

223.5C: Updates reference to revised and retitled OIG Form III-223/1.

223.5G: Adds guidance regarding an exception to required consultation and approval (b) (7)(E)

Appendix B: Updates and renames OIG Form III-223/1.

- 226.1 **Policy.** Statements made by federal employees and non-employees during investigative interviews have substantial value as evidence in criminal prosecutions as well as in civil and administrative proceedings. This chapter establishes policies and procedures for interviewing witnesses and subjects in Office of the Inspector General (OIG) investigations, including the appropriate warnings to be given to interviewees in specified situations. This chapter also establishes procedures for conducting photo lineup displays.
- 226.2 **Reference.** This chapter is issued under the authority contained in the Inspector General Act of 1978, 5 U.S.C. app., as amended and 28 C.F.R. 45.13.
- 226.3 **Scope.** The provisions of this chapter apply to all employees in the OIG Investigations Division.
- 226.4 **General Procedures.** The OIG Investigations Division will ensure that all statements obtained during the course of an investigation are not coerced and are secured through procedures that do not have the appearance of coercion. To that end, appropriate warnings will be given whenever the subject of an investigation is requested to provide evidence pertaining to conduct that may be prosecuted or adjudicated as a criminal, administrative, or civil violation. OIG Special Agents (agents) will inform the interviewee whether the matter being investigated is criminal or administrative and whether the interviewee is a subject or a witness. Further, agents will document all investigative activity by Memorandum of Investigation (MOI), and for certain cases, in lieu of taking a signed sworn statement (affidavit), agents should consider electronically recording the interview. For further details concerning case preparation and recorded interviews, see Inspector General Manual (IGM), Volume III, Chapter 207 (III-207).
- A. **Federal Law and Administrative Decisions.** Agents and supervisors will adhere to all Department of Justice (DOJ) policies and relevant court, Merit Systems Protection Board, and administrative decisions when interviewing federal employees. Agents will adhere to the applicable law and relevant court decisions when interviewing non-employees. Agents and supervisors will maintain their knowledge of current law and administrative decisions regarding interviewing through periodic training and instruction.
- B. **Warnings Before Interview.** Agents will ensure that the federal employees and non-employees they interview during an official investigation are provided the warnings required by the specific circumstances as outlined in this chapter. Agents will also create an accurate record of the warning given at the start of an interview, including a statement that the interviewee understood his or her rights and an indication of whether the warning form was signed.
- C. **Representation.** As prescribed in this chapter, if a DOJ employee requests union representation and the employee reasonably fears disciplinary action or criminal prosecution, agents are required to allow a union representative to be present during an OIG interview.

Except in the custodial situation where the interviewee has invoked his or her right to counsel, the OIG is not required to allow an attorney to be present at an OIG interview. However, it is the OIG's policy to honor an interviewee's request that counsel be present.

If the interviewee is an employee of the FBI and an attorney will be present, the agent should provide an OIG Form 207/9 (IGM III-207, Appendix M) to the attorney and request that the attorney sign it. This form provides that the attorney will not disclose information acquired as a result of his or her representation except under specified circumstances.

In criminal investigations, agents should consult with the prosecutor regarding the applicable rules governing contacts with parties who are represented by counsel. If an agent has questions about this issue in connection with an administrative case or a criminal matter to which no prosecutor is assigned, the agent should contact the OIG Office of General Counsel (OGC).

If an employee who is entitled to a union representative requests both personal counsel and union representation, the agent should allow both to be present.

- D. Instructions to Maintain Confidentiality. At the conclusion of an interview, OIG agents will request that an employee interviewee and, if present, his or her representative not discuss the nature of the interview or investigation with any other persons except the interviewee's counsel.

The DEA has requested that each DEA employee be read and required to sign a specific warning form regarding confidentiality and nondisclosure. OIG agents will use OIG Form III-226/4 (Confidentiality and Nondisclosure) (Appendix A) for this purpose when interviewing any DEA employee.

226.5 Collective Bargaining Agreements and the Role of Employee Unions. Employees of some DOJ components, offices, boards, and divisions (collectively "components") are represented by unions. Collective bargaining agreements have been negotiated between the unions and these DOJ components. Component agency officials are bound by these collective bargaining agreements.

- A. Union Representatives in OIG Interviews. Under the Supreme Court decision in *NASA v. FLRA*, 529 U.S. 229 (1999), OIG investigators are considered "representatives of the agency" as defined in 5 U.S.C. 7114(a) (2) (B), and therefore, OIG agents cannot legally deny a bargaining unit employee's request for union representation during an OIG administrative interview. Although the Supreme Court did not specifically address whether union representation was similarly required if the matter under investigation was criminal, the United States Court of Appeals for the District of Columbia has held that the same rule applies in the criminal context (*DOJ v. FLRA*, 266 F.3d 1228 (2001)). Accordingly, when the

prerequisites (paragraph B below) are met, agents will allow an employee to have a union representative present at an OIG interview, including a criminal interview.

B. Prerequisites for Union Representation at an OIG Interview. A DOJ employee must meet three prerequisites in order to have union representation at an OIG interview:

- (1) The Employee Must Be a Member of a Bargaining Unit. The employee must be an employee of a unit within DOJ for which a union has been certified by the Federal Labor Relations Authority (FLRA) as the exclusive bargaining unit representative. However, the employee is not required to be a member of the union. Examples of bargaining unit employees within DOJ include nonsupervisory, non-agent, and non-attorney personnel in the Justice Management Division and most nonmanagement personnel in the Bureau of Prisons;
- (2) The Employee Must Have a Reasonable Belief That Discipline May Result From the Interview. The right to union representation arises when the circumstances surrounding an interview make it reasonable for the employee to fear that his or her answers might lead to discipline or prosecution. The possibility rather than the inevitability of discipline or prosecution determines the employee's right to union representation.

The subject of an investigation will always meet the reasonable belief test.

A witness who requests union representation should be told that he or she is not the subject of the investigation. The witness should then proceed with the interview without representation. However, the agent will not promise the witness immunity from administrative discipline unless the employing component has previously expressly agreed that the answers provided by the witness or any evidence gained by reason of such answers will not form the basis of disciplinary action.

In some circumstances an employee witness may express a reasonable fear that he or she might be placed in jeopardy as a consequence of what he or she says during an interview and, thus, will be entitled to representation. For example, if a component has a regulation requiring timely reporting of misconduct and a practice of disciplining employees for failure to report, a witness who failed to report misconduct may have a reasonable fear of being disciplined. In such circumstances, a witness's request for union representation will be honored. Agents should consult with the OGC if they have questions about whether a request for union representation must be honored in a particular case; and

- (3) The Employee Must Request Representation. An OIG investigator is not obligated to advise an employee before the start of an interview of his or her right to union representation. Rather, union representation is provided only if

the employee requests it. The employee's request may be made in any manner.

- C. **Role of Union Representative.** Although an employee is not guaranteed the representative of his or her choice, generally an employee has the right to choose his or her union representative. The OIG may postpone an interview for a reasonable period in order to enable a specific representative to be present. However, provided another union representative is available, the OIG is not required to unduly delay an interview until an employee's representative of choice is available. In this situation, inform the employee that he or she must choose another representative.

Except as set forth below, the union may designate anyone to be its representative. The representative need not be a member of the union or a DOJ employee.

In most instances, an OIG agent cannot bar a particular representative, except where the representative is a subject or witness in the investigation whose participation in the interview would undermine the integrity of the investigation. Also, where an investigation involves multiple subjects, the same representative can be prevented from representing more than one subject. The agent should consult with OGC if he or she believes this situation may arise.

Generally, a union representative may clarify questions posed to the employee and provide additional information to assist in the investigation. At the outset of the interview, the interviewing agent will provide the union representative with a copy of OIG Form III-226/6 (Advisory to Union Representative) (see Appendix B) and ask the representative to read and sign the form.

- (1) An agent may demand answers from the employee; the union representative does not have the authority to answer on behalf of the employee or to instruct the employee not to answer. The interviewing agent has the right to hear the employee's own account of the matters under investigation.
- (2) If an employee requests an opportunity to consult with a union representative before answering a question, the agent may: deny that request; demand an answer; and then allow consultation so that the employee can determine whether to modify or supplement his or her response.
- (3) An agent may ask a union representative about the nature of the discussions with the represented employee.
- (4) The agent will deny any request by an employee or his or her representative to electronically record an interview.
- (5) An agent should not interrupt or bar all communications by the union representative during the course of an interview. The representative should be allowed to clarify the agent's questions and clarify an interviewee's

responses. The agent should balance the representative's participation with the orderly flow of the interview and, if requested, allow the representative to ask questions of the employee at the end of the interview.

- (6) The OIG agent will endeavor to avoid a confrontational situation with a union representative. However, if a representative becomes disruptive during the interview, the agent will so inform the employee and provide the employee with OIG Form III-226/7 (Advisory to Employee) (see Appendix C). This form explains that the employee has the option to continue the interview without a representative or forgo the opportunity to be interviewed in connection with the investigation. Examples of disruptive conduct include:
 - a. Repeated objections or arguments for the purpose of interfering with the investigator's ability to complete the interview.
 - b. Coaching the employee to the extent that the representative, rather than the employee, is providing answers.

226.6 Interviews During Criminal Investigations.

- A. Definition of a Subject. The subject of a criminal investigation is someone who is alleged to have engaged in criminal wrongdoing or someone against whom evidence of criminal wrongdoing exists.
- B. Use of Warning Forms. Before beginning the interview, OIG agents will inform an employee subject of his or her rights. A non-employee subject will also be apprised of his or her rights in the circumstances discussed below. Where specific forms are identified later in this chapter, the interviewing agent will read the form aloud to the interviewee, give the interviewee an opportunity to read the form, and ask the interviewee to acknowledge by signature his or her review and understanding of the form.
- C. Refuting Claims of Coercion. An interview may take place if the interviewee refuses to sign the warning form but nevertheless states that he or she understands his or her rights. In such a case, a written record discussing how the warnings were given and that the interviewee acknowledged that he or she understood the warning and agreed to proceed with the interview will be included in the MOI regarding the interview (see also IGM III-207).

Interviewees later may seek to suppress statements made during an interview and claim coercion or fear of termination of employment. The most effective way to refute such claims is evidence prepared at the time of the interview. Such evidence should consist of the interviewee's signature on a warning form or a MOI summarizing the discussion and the interviewee's understanding of the warnings provided.

D. Custodial Interrogation of Subjects.

- (1) Conditions. A custodial interrogation occurs when the interviewee is not free to leave the interview or does not reasonably believe that he or she is free to leave the interview. An interviewee need not be under arrest or incarcerated in order to be in a custodial setting. The location of the interview, a closed or locked door, the length of the interview, and the interviewing agents' behavior, including presence and display of weapons, manner of questioning, and number of agents present, will be considered if an employee raises a judicial challenge to the voluntariness of the interview and admissibility of any statements provided.
- (2) Warning Forms. (The custodial warning forms discussed below can be found in Appendix D.)
 - a. OIG Form III-226/1 (Miranda/Employee) will be used when the subject is a federal employee (non-presidential appointee) and is in custody.
 - b. OIG Form III-226/1a (Miranda/Non-Employee) will be used when the subject in custody is not a federal employee or is a presidential appointee. OIG Form III-226/1b (Miranda/Non-Employee (Spanish Version)) should be used for Spanish speaking non-employees whose command of the English language is in doubt.
- (3) Request for Counsel. In a custodial situation, a subject's request to speak to counsel must be honored by the interviewing agent, who must immediately stop the interview. A subject's request that counsel be present during a custodial interview will also be honored.
- (4) Request for Union Representation. If the prerequisites discussed above are met, a subject's request to have a union representative present at a custodial interview must be honored.

E. Non-Custodial Interrogation of Subjects in Criminal Investigations.

- (1) Conditions. Subjects of investigations of alleged criminal violations are most commonly interviewed by the OIG in non-custodial settings. Because criminal prosecution is possible, the interviewee's participation is voluntary, and he or she is free to leave at any time during the interview. These stipulations must be clearly communicated to the interviewee.
- (2) Warning Form. OIG Form III-226/2 (Non-Custodial Warning/Employee) (Appendix E) will be used when the subject is a federal employee. No specific form is required when the interviewee is not a federal employee, although the agent should orally discuss the voluntary nature of the

interview, the interviewee's freedom to leave, and the fact that any answers or comments may be used against the individual in criminal or other proceedings. When interviewing a presidential-appointee who is the subject of investigation, use OIG Form III-226/5 (Non-Custodial Warning/Presidential Appointee) (Appendix F).

- (3) Request for Counsel. While case law does not demand it, as a matter of OIG policy, the interviewing agent will honor a request that counsel be present during the interview. The counsel may not be another employee of the DOJ or a potential subject or witness in the case.
- (4) Request for Union Representation. If the prerequisites discussed above are met, a subject's request to have a union representative present at a custodial interview must be honored.

F. Interviews of Witnesses. During a criminal investigation, an OIG agent may interview an individual regarding a potential criminal violation committed by another person. If the interviewee has not been given immunity (see section 226.7) and there is no indication that the interviewee is a subject, then the interview is voluntary, and no warning form is required.

When conducting a witness interview, the OIG agent will provide to the witness only the information concerning the investigation necessary for the interview to proceed (that is, the allegation of the investigation and, if pertinent, the subject of the investigation). OIG agents will refrain from discussing the criminal history of the subject. OIG agents will never threaten, verbally abuse, or make unrealistic promises (promises that are not covered by OIG policy or that have not been approved by the prosecuting attorney) to a witness.

- (1) Request for Counsel. While case law does not demand it, as a matter of OIG policy an agent will honor a witness's request that counsel be present during the interview. The counsel may not be another employee of the DOJ or a potential subject or witness in the case.
- (2) Request for Union Representation. As noted above, the right to union representation attaches only in those cases where there is a reasonable possibility that discipline against the interviewee will result from the interview.
- (3) Changing Status: Witness Becomes Potential Subject. Occasionally, an interviewee's answers will indicate that he or she had a significant role in a critical event related to the investigation. If an interviewee's comments or answers suggest that he or she may become a subject in this or another criminal investigation, the agent will interrupt the interview, advise the interviewee of his or her rights as set forth in OIG Form III-226/2 (or 226/5

if the interviewee is a presidential appointee) and proceed only if the interviewee agrees to continue.

226.7 Interviews During Administrative Investigations. Interviews that occur after a criminal declination or in connection with investigations that focus on non-criminal misconduct are considered administrative in nature. In an OIG administrative interview, a DOJ employee is required to answer questions regarding the performance of his or her duties and all related issues.

- A. Definition of a Subject. A subject in an administrative investigation is someone who is alleged to have engaged in non-criminal misconduct or criminal misconduct that has been declined for prosecution or someone against whom evidence of such misconduct exists.

- B. Grants of Immunity. Not all instances of alleged criminal activity will result in criminal prosecution. The factors or guidelines defining when certain instances of illegal conduct will be accepted for prosecution vary from judicial district to judicial district. When a decision has been made to forgo criminal prosecution, an employee is required to answer questions related to his or her official duties. Except in connection with a prosecution for false statements, such compelled statements may not be used in a subsequent criminal prosecution of the interviewee.
 - (1) Declination of Criminal Prosecution. In most instances, an agent will obtain a declination of criminal prosecution from a federal prosecutor before conducting a compelled administrative interview of a subject. A record of the declination, either by a letter from the reviewing prosecutor or an MOI prepared by the agent that identifies the reviewing prosecutor and outlines the details of the consultation, will be placed in the case file.

 - (2) Decision Not to Present Matter for Review. If a Special Agent in Charge (SAC) knows that certain criminal allegations, even if proven, will not satisfy the prosecution standards or guidelines for a particular judicial district, the SAC may choose not to present the matter formally to a federal prosecutor for a prosecutorial decision. A SAC may determine which warnings are appropriate for interviews, which cases must be formally presented for prosecutorial decision, and which cases may be treated as administrative matters without obtaining formal declinations.

- C. Scheduling Administrative Interviews. An administrative interview of an employee normally will be scheduled directly with the employee. However, when necessary, the interviewing agent will schedule the interview through the employee's supervisor to ensure that the employee is on duty and that the supervisor has prior notice for assignment purposes. The agent will specifically inform the supervisor that a non-criminal, administrative interview will be conducted. The agent will also request that the supervisor inform the employee that the interview is an administrative interview and that the employee must attend.

D. Warning Forms.

- (1) Agents will use OIG Form III-226/3 (Warnings and Assurances to Employees Required to Provide Information) (Appendix G) for subjects of administrative investigations. This warning is often referred to as a “*Kalkines* Warning” and includes what is known as the “*Garrity* Warning.” The warnings are based on court decisions discussing the relationship between compelled statements and the Fifth Amendment right against self-incrimination. Witnesses will not in the first instance be compelled to provide a statement. However, agents may use this form for employee witnesses who refuse to be interviewed unless they have been compelled to do so.
- (2) No warning forms are required for non-employee interviewees in administrative investigations.
- (3) See Appendix H for a summary of guidance prescribed for employee interview situations.

E. Scope of Immunity. OIG Form III-226/3 grants derivative use immunity to the interviewee; that is, neither the statements nor information derived from such statements may be used in a subsequent criminal prosecution of the interviewee (except in a false statement prosecution). At the time this warning is presented to an employee, the agent will specifically explain to the interviewee the alleged misconduct about which he or she will be questioned, a requirement in refuting any subsequent challenge as to the scope of the immunity. If an employee begins speaking about other unrelated criminal conduct, the agent will immediately inform the employee that the immunity does not apply to other conduct or admissions. The agent will give the employee a non-custodial warning before questioning him or her about the unrelated conduct.

F. Request for Counsel. If an employee subject requests that counsel be present, the agent generally must honor the request. The agent may deny a request for counsel if there is an identifiable, adverse consequence to the OIG, such as undue delay of the interview or interference with the investigation. What constitutes undue delay will vary depending upon the nature of the investigation, the length of delay, and the agent hardship caused by the delay. Interference may arise from, among other things, an attorney's representation of multiple subjects when the agent believes such representation constitutes a conflict. Before denying a request for counsel, agents should consult with the OGC.

- (1) Counsel's Refusal to Allow Interview. Counsel may attempt to refuse to allow the client employee to participate in an administrative interview. This may be due to counsel's lack of understanding of “use immunity.” The agent will contact OGC in this instance because a letter of explanation from OGC

often will cause the attorney to withdraw a previous instruction to the employee to refuse the interview.

- (2) Counsel's Role During Interview. If counsel is present during an administrative interview, the agent will advise counsel that the employee is obligated to answer questions relating to allegations of work-related misconduct and that any advice by counsel to his or her client not to respond may result in discipline of the employee. This issue should be addressed during the agent's review of the warning form with the employee and the attorney.
 - a. If an employee requests an opportunity to consult with an attorney at any time during the interview, including before answering a question, the agent will honor that request.
 - b. The agent may not ask an employee or an attorney about the nature of their discussions.
 - c. The agent will deny any request by an attorney to electronically record an interview.
 - d. An agent will not interrupt or bar statements by the attorney during the course of an interview. The attorney will be allowed to clarify an agent's questions and may clarify an employee's responses. The agent will balance the attorney's participation with the orderly flow of the interview and, if requested to do so, will allow the representative to ask questions of the employee at the end of the interview.
 - e. If the interviewing agent determines that an attorney is unduly disruptive during the interview, the agent may terminate the interview. The agent should consult with OGC to determine how to proceed following termination of the interview.
- G. Employee Refusal to Cooperate. A DOJ employee may be disciplined for failure to cooperate in an OIG investigation. If an employee refuses to answer questions in an administrative interview, the agent will contact the employee's immediate supervisor and request the supervisor to instruct the interviewee to cooperate.
 - (1) If the supervisor declines to order the employee to cooperate, contact the respective component's internal affairs office either directly or through OIG Headquarters.
 - (2) If the employee continues to refuse to answer questions after being ordered by a supervisor or internal affairs unit to cooperate, take the following actions:

- a. Advise the employee: "Your willful refusal to cooperate in this investigation may be construed as insubordination, which could result in revocation of any security clearance you may hold as well as disciplinary action against you, up to and including dismissal from (name of component)."
 - b. Ask the employee if he or she understands the above advisement and ask the employee if he or she still refuses to answer questions at this time.
 - c. If the employee still refuses to cooperate, end the interview. The events will be noted on the warning form and witnessed by the OIG agents present. The circumstances and witnesses will also be documented in an MOI regarding the attempted interview.
- (3) If the employee continues to refuse, a stronger case for discipline for both insubordination and failure to cooperate will be established by taking the above actions.

H. Off-Duty Conduct. Administrative investigations normally focus on an employee's performance of official duties. However, an employee may be investigated and disciplined for off-duty misconduct if there is a nexus between the offending conduct and the employee's job-related responsibilities so that any proposed discipline would promote the efficiency of the agency.

226.8 Photographic Lineup Displays. A photo lineup is a display of photographs compiled by the investigator for the purpose of exhibiting them to a witness in an effort to positively identify an individual, usually a suspect, who may have committed a crime, aided and abetted in the commission of a crime, or someone whose identity is paramount in some other way to the investigation.

A. Guidelines for Assembly of the Photo Lineup.

(b) (7)(E)



(b) (7)(E)



B. Conducting a Photo Lineup.

- (1) All witnesses will be read the following before they view a photo lineup:

“In a moment I am going to show you a group of photographs. This group of photographs may or may not contain a picture of the person being investigated. Keep in mind that hair styles, beards, and moustaches may be easily changed. Also, photographs may not always depict the true complexion of a person - it may be lighter or darker than shows in the photo. Pay no attention to any markings or numbers that may appear on the photos or any other differences in the type or style of the photographs. When you have looked at all the photos, tell me whether you see any person known to you. Do not tell other witnesses that you have or have not identified anyone.”

(b) (7)(E)



- C. Recording the Identification Process. The agent conducting the photo identification will document the procedure by recording at least the following information in an MOI:

(b) (7)(E)



D. Evidence. The photo identification folder containing all photos and initialed photocopies used in the photo lineup will be processed as evidence as prescribed in IGM III-234.

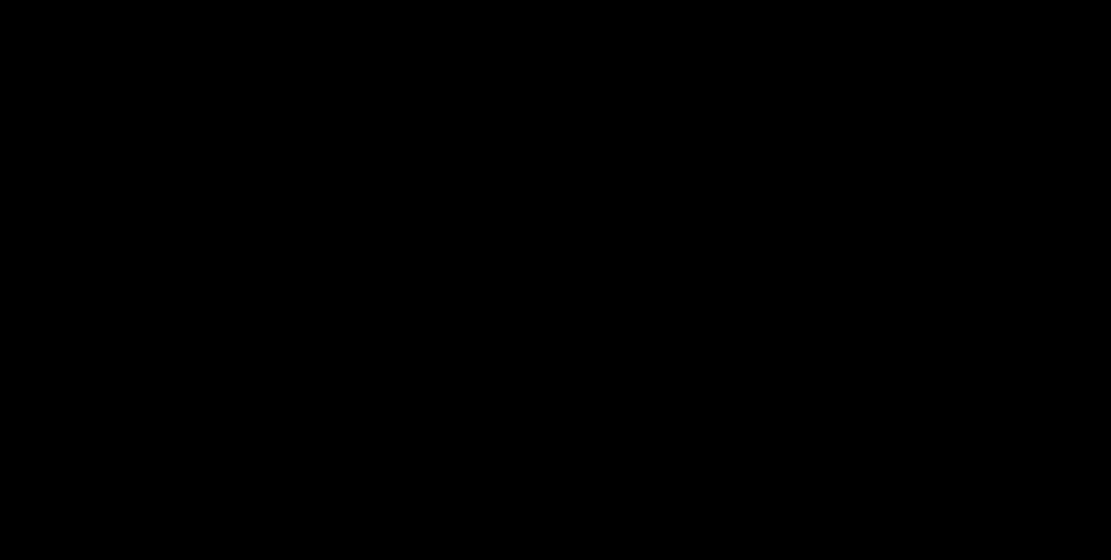
226.9 OIG Office of General Counsel Guidance. The OIG OGC may issue guidance memoranda regarding interview procedures. OGC memoranda will be placed in Appendix I after issuance.

226.10 Interviews of Witnesses and Subjects in OIG Office Space. (b) (7)(E), (b) (7)(F)



A. Instructions Regarding Weapons and Scheduling Interviews. When scheduling an interview, the agent will instruct all subjects and witnesses that they may not bring weapons of any kind into OIG space (knives, firearms, and batons, for example). In addition, the agent will instruct subjects and witnesses to inform their attorneys and union representatives of this weapons prohibition if they will be present at the interview.

B. Admittance of Witnesses into OIG Office Space. (b) (7)(E), (b) (7)(F)




(b) (7)(E), (b) (7)(F)



C. Admittance of Subjects into OIG Office Space. (b) (7)(E), (b) (7)(F)



(b) (7)(E), (b) (7)(F)




226.11 Interviews of Subjects Outside of OIG Office Space.

(b) (7)(E), (b) (7)(F)

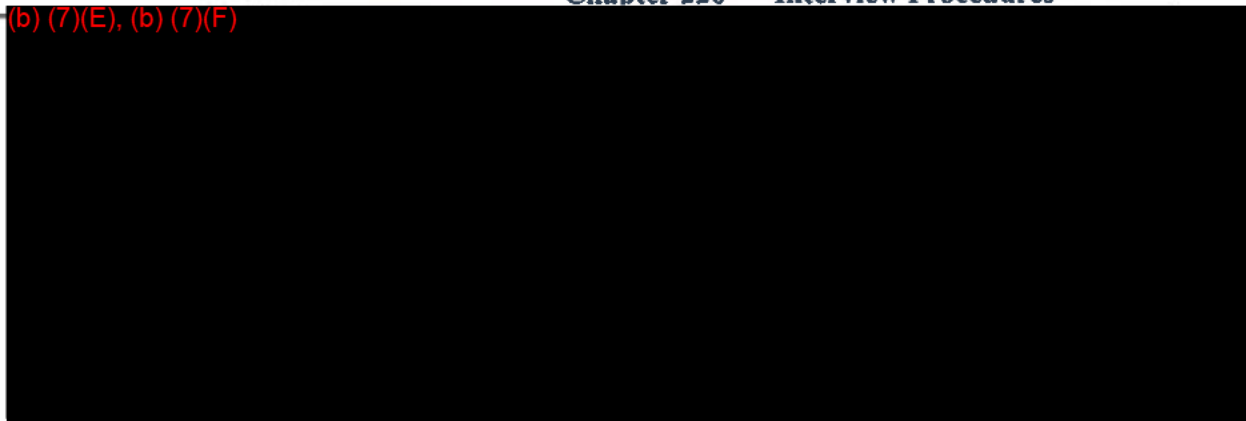


- A. Scheduling of Subject Interviews. When setting up an interview, the agent will instruct all subjects that they may not bring weapons of any kind to the interview (knives, firearms, and batons, for example). In addition, the agent will instruct subjects to inform their attorneys and or union representatives of this weapons prohibition if they will be present at the interview.
- B. Location of the Interview.

(b) (7)(E), (b) (7)(F)



(b) (7)(E), (b) (7)(F)



C. Authority to Modify Policy. (b) (7)(E), (b) (7)(F)



226.12 Rescheduling of Canceled Interviews. If any interview must be canceled because of reasons provided above, the interview will be rescheduled. (b) (7)(E), (b) (7)(F)



226.13 Interviews of Witnesses Outside of OIG Office Space. (b) (7)(E), (b) (7)(F)




226.14 Interviews at Bureau of Prisons Institutions.

A. Accommodation of OIG Agents. (b) (7)(E), (b) (7)(F)



(b) (7)(E), (b) (7)(F)



B. Exceptions to Accommodation of OIG Agents. Because each BOP institution is unique, BOP personnel may not be able to fully accommodate OIG agents as described above. In addition, specific safety issues may preclude BOP personnel from fully accommodating OIG agents.

C. Risks of Being Armed in Administrative Areas. (b) (7)(E), (b) (7)(F)



D. (b) (7)(E), (b) (7)(F)



226.15 Interviews Related to Allegations of Sexual Abuse in Confinement Settings.

A. Victim Interviews.

- (1) In areas that are geographically remote from the nearest OIG office or domicile, initial time-sensitive victim and witness interviews may be conducted by BOP investigators, such as a Special Investigative Supervisor or a Special Investigative Agent, provided that the victim did not make a request for confidentiality in an allegation that he or she reported directly to the OIG. Victims and key witnesses must be interviewed (or re-interviewed) by one or more OIG Special Agents as soon as possible in all open investigations, including those in which such interviews have already been conducted by BOP. Detailed and thorough victim interviews serve the dual benefit of providing additional leads for corroboration and detecting false reporting of sexual assault. (See also Appendix K for definitions of sexual abuse and harassment terms in the Prison Rape Elimination Act.)

- (2) The interviewing agent will make every effort to put the victim at ease and make the victim aware of his or her victim/witness rights, including the right to request a victim advocate.
- (3) The victim is entitled to request a victim advocate to accompany and support the victim through the forensic medical examination process and investigatory interviews and provide the victim with emotional support, crisis intervention, information, and referrals. If the victim requests the presence of a victim advocate, the OIG Special Agent will ensure that such an advocate is available to the victim. To facilitate the logistics of the victim interview if an advocate is requested, the OIG Special Agent shall determine in advance of the interview what arrangements the institution has made (with a local rape crisis center or other community-based organization) to provide victims with access to victim advocates, as required under law, and use such arrangements to provide advocacy services to the victim if requested. If no such arrangements have been made by the institution, or if no advocate is available through the institution's arrangements, the OIG Special Agent shall make reasonable efforts to provide an advocate to the victim upon request. The advocate should be a specialist from a rape crisis center, if available. If a rape crisis center is not available to provide victim advocate services, these services may be provided by a qualified staff member from a community-based organization, or if no outside services are available, a qualified staff member of the institution or component, such as a staff psychologist who has been screened by the component for appropriateness to serve in that role.
- (4) Prior to the conclusion of the interview, the OIG Special Agent should make every effort to ensure that the victim has described the facts of the assault(s) in specific, clear terms that address the legal elements of the crime.
- (5) (b) (7)(E), (b) (7)(F)
- (6)
- (7) Victim interviews may be documented with a MOI, an affidavit, or an audio or video recording with proper approvals. (b) (7)(E)
(b) (7)(E)

- B. Subject Interviews. All investigations with evidence that appears to support criminal prosecution will be presented to the U.S. Attorney's Office with jurisdiction. No compelled interviews will be conducted in connection with such a case without the concurrence or a prosecutorial declination from an Assistant U.S. Attorney.

APPENDIX A

**Acknowledgment of Directive to Maintain
Confidentiality and Nondisclosure
(Required for DEA Employees)**

(OIG Form III-226/4)

This form may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

Acknowledgment of Directive to Maintain Confidentiality and Nondisclosure

You have been interviewed by _____

and _____ of the Department of Justice, Office of the Inspector

General, concerning _____

Under the authority of the DEA Planning and Inspection Manual, "Chapter 83, Internal Investigation," Subchapter 8302 (D) (7), you are hereby directed not to disclose to anyone, except your attorney, or union representative, that:

1. You have been interviewed by the Office of the Inspector General concerning this matter, and
2. The fact that the Office of the Inspector General is conducting an investigation into this matter.

Failure to comply with this directive may be grounds for administrative action against you.

ACKNOWLEDGMENT

I have read the above directive and agree to keep such information confidential.

Office of the Inspector General
Special Agent Conducting Inquiry

Subject's Signature

Witness

Subject's Printed Name

Time, Date, and Place

APPENDIX B

Advisory to Union Representatives

(OIG Form III-226/6)

This form may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

ADVISORY TO UNION REPRESENTATIVES

A Department of Justice Employee has requested that you participate as a union representative in an interview being conducted by the Office of the Inspector General of the Department of Justice (OIG). The interview is part of an official investigation being undertaken pursuant to the OIG's authority under the Inspector General Act, as amended.

The OIG is conducting this interview in order to obtain the employee's account of the matters under investigation. The OIG understands that you are entitled to assist the employee during the course of the interview and may pose questions and attempt to clarify issues. In order to facilitate your representation of the employee, you will be afforded a reasonable opportunity to confer with the employee during the course of the interview.

The OIG expects that you will refrain from any action that would interfere with the OIG's legitimate interest in achieving the objectives of this investigation or would compromise its integrity. The OIG is interested in obtaining the employee's own account of the matters under investigation. Accordingly, please do not attempt to answer questions on behalf of the employee, dictate the employee's answers to questions asked, or otherwise to take charge of this proceeding. In order to maintain the integrity of this investigation, the OIG requests that you not reveal to anyone not present at this proceeding the purpose of this interview or the questions asked and answers provided.

We expect that any disagreement regarding this interview, or your roles as a union representative, will be resolved amicably during the course of this proceeding. However, in order to avoid an adversarial confrontation and to achieve the objectives of the investigation, the OIG reserves the right to (1) terminate the interview or (2) afford the employee the choice of either proceeding without your participation or foregoing the opportunity to be interviewed in this matter.

CERTIFICATION

I hereby certify that _____ appeared at an official OIG investigative interview as a union representative and was provided a copy of this Advisory.

Name of OIG Special Agent

Date

APPENDIX C

**Advisory to Employee After Union Representative Interference
With OIG Interview**

(OIG Form III-226/7)

This form may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

ADVISORY TO EMPLOYEE

During an interview undertaken as part of an official Department of Justice Office of the Inspector General (OIG) investigation, the individual serving as your union representative has been advised that he or she has engaged in activity that has interfered with the OIG's legitimate interest in achieving the objective of the investigation. In order to avoid an adversarial confrontation and to achieve the objectives of the investigation, you are being afforded the choice of (1) continuing this interview without the participation of your union representative or (2) discontinuing the interview, thereby forgoing the opportunity to be interviewed in connection with this matter. You will not be subject to discipline for failure to cooperate in this investigation if you choose to discontinue the interview.

ACKNOWLEDGMENT

Having read this advisory, I choose to:

_____ Continue with the OIG interview without the participation of a union representative.

_____ Forego the opportunity to be interviewed in connection with this investigation.

Employee Signature

Date

APPENDIX D

Miranda Warnings for Custodial Situations

OIG Form III-226/1
OIG Form III-226/1a
OIG Form III-226/1b

These forms may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

YOUR RIGHTS

Before we ask you any questions or you make any statement, you must understand your rights.

- You have the right to remain silent and refuse to answer any questions at any time.
- Anything you say or do can be used against you in a court of law or other proceedings.
- You have the right to talk to a lawyer for advice before answering any questions and to have a lawyer with you during any questioning now or in the future.
- If you cannot afford a lawyer, one will be provided for you without cost.
- If you decide to answer questions now, you have the right to stop answering questions at any time you desire.
- If you refuse to answer the questions posed to you on the grounds that the answers may tend to incriminate you, no disciplinary action will be taken against you for remaining silent.

I have read this statement of my rights and I understand what my rights are. I am willing to make a statement and answer questions. I understand and know what I am doing. No promises or threats have been made to me, and no pressure or coercion of any kind has been used against me.

Office of the Inspector General
Special Agent Conducting Inquiry

Subject's Signature

Witness

Date

Time

Place

UNITED STATES DEPARTMENT OF JUSTICE

Office of the Inspector General

YOUR RIGHTS

Before we ask you any questions or you make any statement, you must understand your rights.

- You have the right to remain silent and refuse to answer any questions at any time.
- Anything you say can be used against you in a court of law or other proceedings.
- You have the right to talk to a lawyer for advice before answering any questions and to have a lawyer with you during any questioning now or in the future.
- If you cannot afford a lawyer, one will be provided for you without cost.
- If you decide to answer questions now, you have the right to stop answering questions at any time you desire.

I have read this statement of my rights and I understand what my rights are. I am willing to make a statement and answer questions. I understand and know what I am doing. No promises or threats have been made to me, and no pressure or coercion of any kind has been used against me.

Office of the Inspector General
Special Agent Conducting Inquiry

Subject's Signature

Witness

Date

Time

Place

Departamento De Justicia De Los Estados Unidos

Oficina del Inspector General

NOTIFICACION DE LOS DERECHOS "MIRANDA" EN LOS CASOS DE CUSTODIOS QUE NO SEAN EMPLEADOS DEL DEPARTAMENTO

Advertencias y garantías de los custodios

SUS DERECHOS

Antes de que le hagamos cualquier pregunta o de que Usted haga cualquier declaración, debe conocer sus derechos:

- Usted tiene el derecho al silencio y a negarse a responder a las preguntas que se le hagan en cualquier momento.
- Lo que diga o haga puede utilizarse contra Usted en un tribunal o en cualquier otro procedimiento judicial.
- Usted tiene el derecho a consultar con un abogado antes de responder a cualquier pregunta y de estar acompañado de un abogado en cualquier interrogatorio que se le haga ahora o en el futuro.
- Si no puede pagar a un abogado, se le facilitará uno gratuitamente.
- Si decide responder ahora a las preguntas, tiene el derecho a negarse a responder en cualquier momento que lo desee.

He leído esta declaración y entiendo cuáles son mis derechos. Estoy dispuesto a hacer una declaración y a responder a las preguntas. Comprendo y sé lo que estoy haciendo. No me han hecho ninguna promesa ni amenaza, ni nadie me ha hecho presión ni coacción de ninguna forma.

Oficina del Inspector General
Agente Especial que realiza la indagacion

Firma del Sujeto

Testigo

Fecha

Hora

Lugar

APPENDIX E

**Warnings for Non-Custodial
Situations – Federal Employees**

(OIG Form III-226/2)

This form may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

**WARNINGS AND ASSURANCES TO EMPLOYEE REQUESTED
TO PROVIDE INFORMATION ON A VOLUNTARY BASIS**

You are being asked to provide information as part of an investigation being conducted by the Office of the Inspector General. This investigation is being conducted pursuant to the Inspector General Act of 1978, as amended.

This investigation pertains to:

This is a voluntary interview. Accordingly, you do not have to answer questions. No disciplinary action will be taken against you if you choose not to answer questions.

Any statement you furnish may be used as evidence in any future criminal proceedings or agency disciplinary proceeding, or both.

WAIVER

I understand the warnings and assurances stated above and I am willing to make a statement and answer questions. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me.

Office of the Inspector General
Special Agent

Employee's Signature

Witness

Date

Time

Place

APPENDIX F

Warnings for Non-Custodial Situations – Presidential Appointees

(OIG Form III-226/5)

This form may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

**WARNINGS AND ASSURANCES TO EMPLOYEE REQUESTED
TO PROVIDE INFORMATION ON A VOLUNTARY BASIS**

You are being asked to provide information as part of an investigation being conducted by the Office of the Inspector General. This investigation is being conducted pursuant to the Inspector General Act of 1978, as amended.

This investigation pertains to: _____

This is a voluntary interview. Accordingly, you do not have to answer questions.

Any statement you furnish may be used as evidence in any future criminal proceedings or agency disciplinary proceeding, or both.

WAIVER

I understand the warnings and assurances stated above and I am willing to make a statement and answer questions. No promises or threats have been made to me, and no pressure or coercion of any kind has been used against me.

Office of the Inspector General
Special Agent

Employee's Signature

Witness

Date

Time

Place

APPENDIX G

Warnings and Assurances to Employees Required to Provide Information

(OIG Form III-226/3)

This form may be reproduced

UNITED STATES DEPARTMENT OF JUSTICE
Office of the Inspector General

**WARNINGS AND ASSURANCES TO EMPLOYEE REQUIRED
TO PROVIDE INFORMATION**

You are being asked to provide information as part of an investigation being conducted by the Office of the Inspector General. This investigation is being conducted pursuant to the Inspector General Act of 1978, as amended.

This investigation pertains to _____

You have a duty to reply to the questions posed to you during this interview and agency disciplinary action, including dismissal, may be undertaken if you refuse to answer or fail to reply fully and truthfully.

Neither your answers nor any information or evidence gained by reason of your answers can be used against you in any criminal proceeding. However, if you knowingly and willfully provide false statements or information in your answers, you may be criminally prosecuted for that action. The answers you furnish and any information or evidence resulting from them may be used in the course of agency disciplinary proceedings.

ACKNOWLEDGMENT

I have read and understand my rights and obligations as set forth above.

Office of the Inspector General
Special Agent

Employee's Signature

Witness

Date

Time

Place

APPENDIX H

Guide for Employee Interview Situations

EMPLOYEE INTERVIEW AND FORM GUIDE

	Custodial Interrogation	Non-Custodial Criminal Interview	Administrative Interview
OIG form	III-226/1	III-226/2 or III-265/5 (Presidential Appointees only)	III-226/3
Employee participation	Voluntary	Voluntary	Required
Employee request for counsel	Agent must allow counsel; cease questioning until counsel is present.	Agent should honor request that counsel be present.	Agent should honor request that counsel be present.
Employee request for union representation	Agent must allow union representation if bargaining unit employee requests representation.	Agent must allow union representation if bargaining unit employee requests representation.	Agent must allow union representation if bargaining unit employee requests representation.

FORM SUMMARY

OIG Form III-226/1

Miranda Warning for Custodial Situations - Federal Employees

This form should be used in those situations where an employee is under arrest or subject to "custodial interrogation" (*Miranda v. Arizona*, 384 U.S. 436, 444 (1966)). The principal factor is whether an objective or reasonable person in the interviewee's position would believe he/she was in custody under the circumstances, that is, not free to leave or subject to a restraint on movement equivalent to formal arrest. A court will consider where the interrogation occurred; how long it lasted; how many officers or interviewers were present; what was said and the manner of delivery; what, if any, physical restraints were used on a person or were present (e.g., presence or use of a gun, handcuffs, guard at door); and whether the interviewee was free to leave or placed under arrest after the interview (*United States v. Griffin*, 922 F.2d 1343 (8th Cir. 1990); *United States v. Mitchell*, 763 F. Supp. 1262 (D. Vt. 1991)).

OIG Form III-226/1a**Miranda Warning for Custodial Situations - Non-Employees and Presidential Appointees**

This form should be used when an individual is under arrest or subject to “custodial interrogation,” as described above. Note that this form is used for persons who are not employees or for presidential appointees; Form 226/1 is used for employees. The significant difference in the text is that employees are notified that they cannot be discharged simply for exercising their Fifth Amendment right to remain silent. OIG Form III-226/1b is a Spanish language version of the 226/1a.

OIG Form III-226/2**Warning for Non-Custodial Situations - Federal Employees**

This form is used when a subject is being questioned on a voluntary basis. The allegations may concern potential criminal behavior, civil wrongdoing, or an administrative violation. The critical elements for this form are that the interviewee is a potential subject of the investigation; criminal prosecution is a possibility; prosecution has not been declined; and the interview is voluntary. In this situation, it is critical that an agent emphasize the voluntary nature of the interview and the employee's right to end the interview and leave at any time.

Please note that no similar form is required when the subject of an investigation who is not an employee is interviewed on a voluntary basis. It is essential, however, that the agent verbally advise the subject of the voluntary nature of the interview and the person's right to leave at any time.

OIG Form III-265/5**Warning for Non-Custodial Situations – Presidential Appointees**

This form should be used when the individual being questioned is a presidential appointee. The allegations may concern potential criminal behavior, civil wrongdoing, or an administrative violation; the interviewee is a potential subject of the investigation; criminal prosecution is a possibility and prosecution has not been declined. The interview is voluntary and the interviewee retains the right to end the interview and leave at any time. The significant difference in the text is that the presidential appointee can be discharged solely for remaining silent.

OIG Form III-226/3**Warnings and Assurances – Employee Required to Provide Information**

This form is commonly referred to as the *Kalkines* warning, based on the case *Kalkines v. United States*, 473 F.2d 1391 (Ct. Cl. 1973). This form is used when prosecution has been declined or the investigation is otherwise non-criminal in nature and the interviewee is an employee subject. In this instance, the employee is required to participate in the interview and may be disciplined for failing to cooperate. This form may also be used for off-duty misconduct interviews. This form may also be used for employee witnesses who refuse to provide a statement unless compelled to do so.

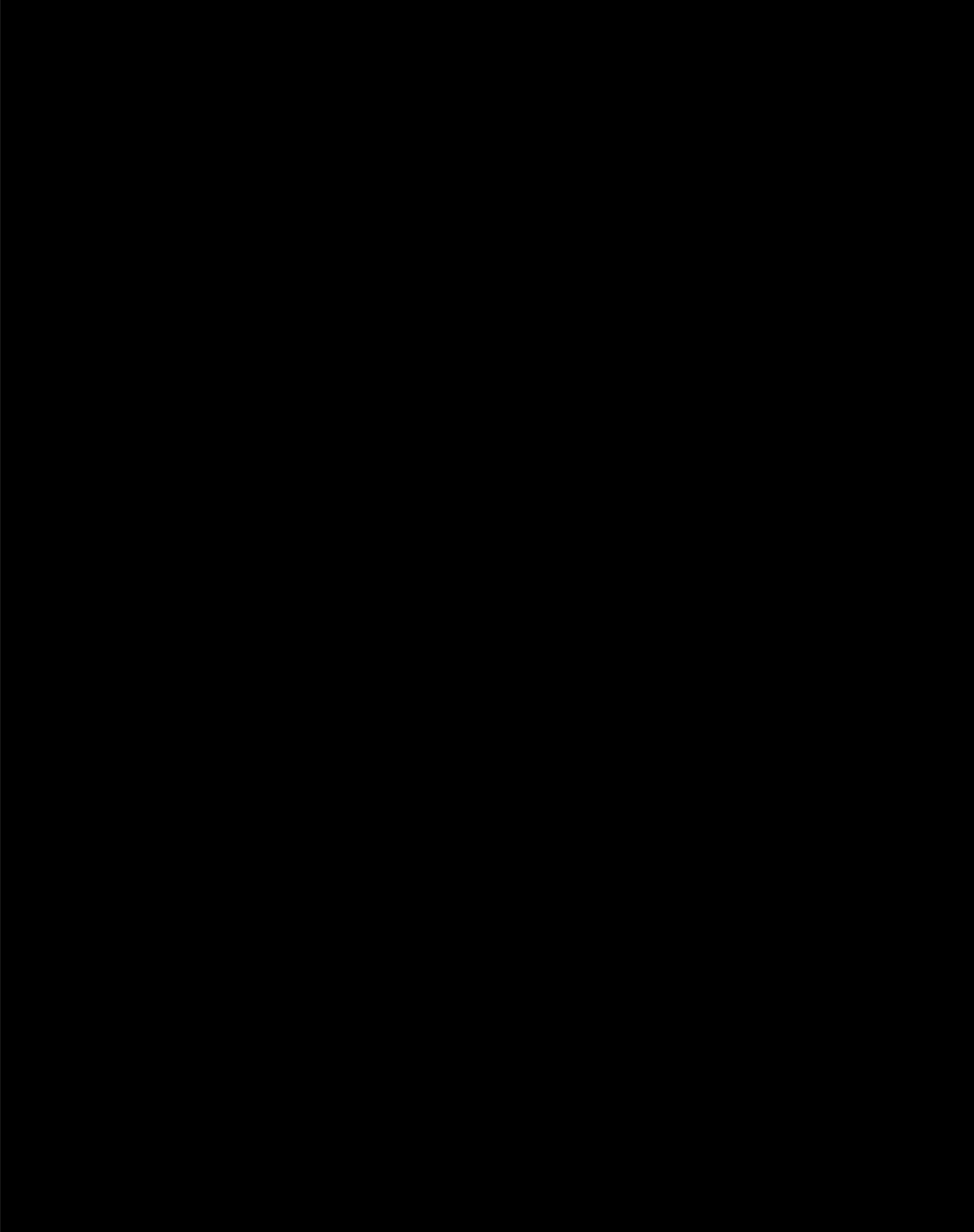
APPENDIX I

**OIG Office of General Counsel Memoranda
Relative to Interview Procedures**

(Agents: Place OGC-issued memoranda behind this appendix page.)

APPENDIX J

Accommodation Requests by OIG Investigators





APPENDIX K

Definitions of Terms in the Prison Rape Elimination Act

DEFINITIONS OF TERMS IN THE PRISON RAPE ELIMINATION ACT

The definition of *sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer* includes any of the following acts, with or without consent of the inmate, detainee, or resident:

- (1) contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) contact between the mouth and the penis, vulva, or anus;
- (3) contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (4) penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (5) any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (6) any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1)-(5);
- (7) any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of an inmate, detainee, or resident, and
- (8) voyeurism by a staff member, contractor, or volunteer.

Voyeurism by a staff member, contractor, or volunteer means an invasion of privacy of an inmate, detainee, or resident by staff for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring an inmate to expose his or her buttocks, genitals, or breasts; or taking images of all or part of an inmate's naked body or of an inmate performing bodily functions.

Sexual harassment in a confinement setting includes:

- (1) repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- (2) repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 226
Interview Procedures
Revisions

This chapter was previously revised on April 23, 2007, and originally issued on May 19, 1997. This chapter was rewritten to reflect updates and/or changes in policies, laws, and guidelines.

This chapter revision consists of an update to OIG Form III-226/1 (Miranda-Employee) in Appendix D to ensure that the Garrity warning on this form is consistent with the Garrity warning on OIG Form III-226/2 (Non-custodial/Employee).

This chapter was previously revised to include an inserted revised policy, approved by the Inspector General or his Designee, issued July 9, 2014:

This policy addition is in conformance with the Prison Rape Elimination Act (PREA), Public Law 108-79, which was passed unanimously by Congress in 2003, and AG Order No. RIN 1105-AB34, as codified in the Code of Federal Regulations (C.F.R.), Title 28, Part 115, on May 16, 2012. (See also www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf.)

226.15: Adds guidance concerning processing and investigation of allegations of sexual abuse in confinement settings (Policy Memorandum FY 14-POL-03).

Appendix K: Adds Definitions of Terms in the Prison Rape Elimination Act (Policy Memorandum FY 14-POL-03).

Changes, additions, and deletions in guidance issued April 22, 2009, appear in the following sections.

226.10: Adds new guidance regarding witness and subject interviews conducted in OIG office space, including weapons instructions when scheduling interviews and admittance to the OIG premises.

226.11: Adds new guidance regarding subject interviews conducted outside of OIG office space.

226.12: Adds new guidance regarding site requirements of interviews that are rescheduled.

226.13: Adds new guidance regarding witness interviews conducted outside of OIG office space.

226.14: Adds guidance regarding safety and assistance when OIG interviews are conducted at BOP institutions.

Appendix J: Adds the BOP memorandum issuing safety and assistance guidance related to OIG investigative activities.

- 230.1 **Policy.** This chapter establishes Office of the Inspector General (OIG) policies and procedures to apply for, obtain, and serve subpoenas for use in OIG investigations. The Inspector General (IG) subpoena is a powerful investigative tool and is to be used with care (b) (7)(E)
- A. IG subpoenas will be issued in full compliance with all applicable federal laws, including the Right to Financial Privacy Act (12 U.S.C. § 3401-3422); the Fair Credit Reporting Act (15 U.S.C. § 1681), and the Electronic Communications Privacy Act (18 U.S.C. §§ 2701-2712).
- B. IG subpoenas compel the production of records and documents. IG subpoenas do not compel testimony.
- C. Consideration will be given to reasonable requests by a record custodian for extra time to gather the subpoenaed material and to alternative accommodations regarding inspection and copying.
- 230.2 **Reference.** This chapter is issued under the authority contained in the Inspector General Act of 1978, 5 U.S.C. app., as amended.
- 230.3 **Scope.** Provisions of this chapter apply to all employees in the OIG Investigations Division (INV).
- 230.4 **General Procedures.** IG subpoenas are issued by one of two methods.
- A. Subpoenas seeking subscriber and user information (not communication content) from communications carriers and records from utility companies, hotels/motels, or rental car companies (and in Federal Bureau of Prisons cases only, from Western Union or similar entities) may be issued directly by field offices.
- B. All other subpoena requests will be made through the OIG Office of General Counsel (OGC) and, upon favorable OGC recommendation, issued by the IG or the Deputy Inspector General (DIG).
- 230.5 **INV-Issued Subpoenas.** Authority is delegated to field and headquarters Special Agents in Charge (SAC) and the Chief of the Digital Forensics and Technology Investigations Unit (DFTIU) to issue subpoenas requesting subscriber and user information (but not content) from telephone companies, paging services, and Internet service providers; occupancy records from hotels and motels; company records of utility providers; and car rental records. In Federal Bureau of Prisons investigations only, the SAC is delegated the authority to issue subpoenas to Western Union (or similar entities) for money order information. This authority may be exercised by an employee serving as an acting SAC but may not be further delegated. All references to SAC in this chapter are inclusive of the

Chief, DFTIU. The Assistant Inspector General for Investigations and the Deputy Assistant Inspector General for Investigations also have authority to issue INV-issued subpoenas.

- A. Sensitive Targets Exception. Sensitive targets are excepted from INV-issued subpoena procedures. A request for a subpoena directed to a communication carrier, car rental company, public utility, or hotel or motel and seeking information regarding any of the following sensitive target persons or entities will be submitted to OGC for review and approval by the IG or the DIG:
- (1) an attorney, law firm, or paralegal;
 - (2) a federal judge, a Member of Congress, a member of the executive branch at executive level IV or above, or a person who has served in such capacity within the previous 2 years;
 - (3) an employee of a foreign government;
 - (4) (b) (7)(E)
 - (5) a member of a media organization; and
 - (6) any other subpoenas that a SAC believes may raise special or sensitive concerns.
- B. Reimbursement Requests. Any invoice or question by a communications carrier, car rental company, utility company, or hotel or motel regarding reimbursement for compliance with a subpoena will be referred to the OIG Management and Planning Division, which will in turn consult with OGC if needed.
- C. Nondisclosure. SACs have the authority to request that recipients of Division-issued subpoenas not disclose the existence of the subpoena to their subscriber or customer. Any issues regarding the time period of nondisclosure will be referred to OGC.
- D. Telephone and Internet Requests Beyond Basic Subscriber Information. If a subpoena request for information from a telephone company or Internet service provider goes beyond what is listed as basic subscriber information, field offices will submit the IG subpoena to OGC for review and approval or use another means, such as a grand jury subpoena or search warrant.

230.6 INV-Issued Subpoena Procedures. The following documents constitute the INV-issued subpoena package -- cover letter to the recipient of the subpoena; subpoena; return of service; attachment designating the records being requested (if necessary); Privacy Act statement; and certificate of compliance:

- A. Cover Letter. The cover letter will show the name and address of the recipient; the name, address, and telephone number of the agent seeking the records; and the name of the SAC issuing (signing) the subpoena. (See Appendix A for a cover letter example.)

The cover letter states that the subscriber or customer should not be notified of the existence or contents of the subpoena until further notice. (b) (7)(E)

(b) (7)(E)



- B. Subpoena. OIG Form III-230/2 (Subpoena Duces Tecum) is mandatory for a field-issued subpoena and customizable. See Appendix B. (See also the OIG Intranet Investigations Division home page for a fillable OIG Form III-230/2 that is ready for subpoena use for telephone and Internet service subscriber information.)

Each subpoena must include the following information:

- (1) the name of the Special Agent and office location (street address);
 - (2) the date and time records should be produced (generally 30 days from the date of service);
 - (3) description of the general nature of the investigation; care must be given to ensure that this description meets the nature of the investigation;
 - a. The typical description of the investigation is “an investigation into allegations of misconduct by a DOJ employee.” Do not specify that the subject is employed by a particular component.
 - b. Other common alternatives are:
 - “An investigation into allegations of misconduct by a former DOJ employee.”
 - “An investigation into allegations of misconduct by a contractor or subcontractor to DOJ.”
 - (4) description of documents sought (alternatively, you may provide this information on an attachment); and
 - (5) the subpoena number.
- C. Return of Service. Return of service information will be completed when the agent serves the subpoena. Refer to Appendix C and Section 230.9 below for detailed instructions.)

- D. Subpoena Attachment. While some subpoenas seek limited information, such as subscriber data, many also seek information regarding subscriber, tolls, local calls, and related services, and the information detailing the request may not fit in the space provided on the subpoena itself. Appendix D contains sample language for subpoenas directed to communications carriers, utility companies, car rental agencies, hotels/motels, and Western Union. The sample wording may be modified to meet particular needs.
- E. Privacy Act Statement. The Privacy Act statement is a standardized document that will accompany all subpoenas. No modifications are appropriate or necessary. (See Appendix E.)
- F. Certificate of Compliance. The wording of the compliance certification will not be modified except to reflect the number and the date of the subpoena. (See Appendix F.)
- G. Approval of Subpoena. The requesting agent must complete and submit a subpoena application, the subpoena itself, and all related documents to the SAC for review, approval, and signature. (See Appendix G for application request and subpoena package checklist samples.)
- H. Subpoena Numbering System. Given that each field office SAC has authority to issue subpoenas, each office will use a numbering system that includes a unique identifier for that office.
- (1) Numbering will begin anew each fiscal year and must use the following format:
- Chicago Field Office: CFO-FY06-1, CFO-FY06-2; CFO-FY07-1
Dallas Field Office: DFO-FY06-1, DFO-FY06-2; DFO-FY07-1
Denver Field Office: DVFO-FY-06-1, DVFO-FY06-2; DVFO-FY07-1
Fraud Detection Office: FDO-FY06-1, FDO-FY-06-2; FDO-FY07-1
Los Angeles Field Office: LAFO-FY06-1, LAFO-FY06-2; LAFO-FY07-1
Miami Field Office: MFO-FY06-1, MFO-FY06-2; MFO-FY07-1
New York Field Office: NYFO-FY06-1, NYFO-FY06-2; NYFO-FY07-1
Washington Field Office: WFO-FY06-1, WFO-FY06-2; WFO-FY07-1
Digital Forensics and Technology Investigations Unit: DFTIU-FY13-1
- (2) OGC will use a separate numbering system for subpoenas issued through OGC.
- I. Recordkeeping. Each office shall maintain a log of subpoenas to facilitate any search or review of issued subpoenas and to use as samples for preparation of future subpoenas. This log will include the number of the subpoena, the date the subpoena was issued, to whom the subpoena was issued, the case agent, case number, and the subject of the investigation. (See Appendix H.)

230.7 OGC-Issued Subpoenas. All requests for OIG subpoenas, other than those described above must be made through OGC.

A. Requesting the Subpoena. OIG Special Agents (agents) prepare the subpoena request. (See Appendix I.) OGC will prepare the subpoena itself, notification documents, and cover letter. After review and approval by the SAC, the field office will forward the subpoena request via e-mail to OGC. OGC will review the request for completeness, validity, and legality. Upon OGC's favorable recommendation, the IG or DIG will issue the subpoena. Central control and inventory of IG or DIG issued subpoenas is maintained by OGC.

- (1) A subpoena will not be requested until attempts have been made to obtain the information by other means. For example, if a document or record is available under the audit clause of a contract or if an individual or entity otherwise has a contractual obligation to provide certain documents, attempts will be made to obtain the documents by reference to that authority.
- (2) Agents and supervisors will consult with OGC as early as possible when considering the use of an OIG subpoena. Such early consultation can significantly assist in determining alternate means of acquiring needed materials, as well as assist in framing and processing the subpoena request and the subpoena.
- (3) Should it be necessary to obtain judicial enforcement of an OIG subpoena, the government must establish that the documents sought are reasonably relevant to a legitimate OIG inquiry and that the demand for documents is neither unduly burdensome nor overly broad. Judicial enforcement of an OIG subpoena will be coordinated between OGC and the appropriate United States Attorney's Office (USAO) in the judicial district where the enforcement action will be initiated.

B. Financial Institutions and Credit Card Issuers.

- (1) Records sought from financial institutions and credit card issuers regarding an individual or small partnership are subject to the Right to Financial Privacy Act (RFPA). The Act requires either simultaneous customer notice that his or her financial records are being sought or a court order to delay notice to the customer (12 U.S.C. §§ 3405, 3409). Copies of the subpoena and related forms must be provided to both the financial institution and the customer. Also, a waiting period is imposed before the subpoena takes legal effect, allowing for the customer to file a judicial challenge.
- (2) If an agent wishes to delay notice to a customer, OGC, in consultation with the agent, will prepare a declaration, motion, memorandum, and proposed order for filing with the court by the appropriate USAO.

- C. Credit Reporting Services. Under the Fair Credit Reporting Act (15 U.S.C. § 1681b), a grand jury subpoena or court order must be issued if a government agency is seeking an individual's credit history or related information as part of an investigation. OGC will prepare, with the agent's assistance, the necessary documents for filing by the appropriate USAO.
- D. Telephone Companies and Internet Service Providers. The Electronic Communications Privacy Act (ECPA), 18 U.S. C. §§ 2701-2712, regulates how the government can obtain stored customer or subscriber records from Internet service providers and telephone companies. OIG subpoenas may be used to obtain basic account information without notice to the subscriber. Basic account information means: (a) name; (b) address; (c) local and long distance telephone connection records (or records of session times and durations); (d) length of service (including start date) and types of service utilized; (e) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (f) means and source of payment for such service (including any credit card or bank account number). As noted in Section 230.5 above, SACs are authorized to issue subpoenas to telephone companies and Internet service providers that seek this basic account information. However, requests that seek any information beyond the basic subscriber information must be submitted to OGC.
- E. Internal Revenue Service. A court order is necessary to obtain federal tax returns and taxpayer information (26 U.S.C. § 1603). OGC will work with the appropriate USAO to obtain an ex parte court order.
- F. State or Public Agencies. State or public agencies have periodically asserted that they are not authorized to release information pursuant to a state government privacy statute. If such assertions are made when an agent makes a preliminary inquiry regarding access to records, the agent will contact OGC, which may be able to resolve these concerns without litigation before the issuance of a subpoena.
- G. Federal Agencies. DOJ entities are required by the Inspector General Act of 1978, as amended, to provide, without subpoena, relevant documents requested in connection with an OIG investigation. Although other federal agencies are also expected to cooperate with DOJ IG, the Inspector General Act does not allow any OIG to subpoena records from any federal agency (5 U.S.C. app. § 6(a)(4)). If an agent finds that a DOJ entity or other federal agency is reluctant to provide the requested information, the agent will contact OGC.

230.8 Service of Subpoenas. Service of OIG subpoenas will be made as soon as practicable following issuance. In the event the subpoena is not served within 3 working days after issuance or receipt by the field office, OGC will be notified prior to serving the subpoena.

- A. Personal Service Preferred. Subpoenas will be served during reasonable hours by the most practical method under all circumstances. Personal delivery to the

addressee is preferable and must be attempted in any situation where refusal to comply with the subpoena is reasonably anticipated.

B. Additional Acceptable Methods of Service.

- (1) Service Upon an Individual. In lieu of service by personal delivery of the subpoena to the addressee, an agent may deliver the subpoena at the addressee's residence or usual dwelling place to a person who is at least 18 years of age and who resides at that location or personally deliver the subpoena to an agent authorized by law to receive service of process for the individual named in the subpoena. When served by delivery to an agent, a copy of the subpoena will also be sent by registered mail (return receipt requested) to the addressee's residence.
- (2) Service Upon a Corporation, Partnership, or Unincorporated Association. Service upon a corporation, partnership, or unincorporated association will be made during normal business hours and upon the addressee named in the subpoena. If the addressee is unavailable, then service will be effected on any officer, partner, managing or general agent, or any other agent authorized by law or appointment to receive service of process. When the subpoena is served on an authorized agent, a copy of the subpoena also will be sent by registered mail (return receipt requested) to the organization's place of business.
- (3) Service Upon a State Government or Municipal Corporation or Other Non-Federal Government Organization. Service upon a state government or municipal corporation or other non-federal government organization will be effected by delivery of the subpoena to the chief executive officer of the organization or by any other means for service of process that is prescribed by the law of the state.
- (4) Service by Registered or Certified Mail, Facsimile, or Federal Express. Service by registered or certified mail, facsimile, or Federal Express is the least desirable method, especially where resistance to the subpoena is expected. However, it may be used when no other method is practicable or when the intended recipient offers to accept service by this method and when no resistance to the subpoena is expected (such as is frequently the case with communications carriers).
- (5) Financial Institutions and Financial Institution Customers. A subpoena will be personally served on a financial institution. In addition, the RFPA requires that a copy of the subpoena and accompanying notices be provided to the customer unless a court order for delay of notice has been obtained. The RFPA permits these documents to be mailed to the customer in lieu of personal delivery. In such cases, mailing will be done by registered or certified mail, return receipt requested, or by Federal Express.

- C. Receipts. If service is made on a person other than the person named in the subpoena, the OIG agent will either obtain a receipt or ask the person to acknowledge receipt on the “Return of Service” section on the back of the agent's copy of the subpoena. The recipient's title (if any) and the relationship of the recipient to the subpoenaed party will be indicated.
- D. Attorneys. Upon receipt of a timely request by a subpoenaed party, subpoenas may be served upon an attorney of record for the party or entity named in the subpoena. Prior to or concurrent with the service of a subpoena upon the attorney of record, the attorney will be requested to confirm in writing that he or she is authorized to accept the subpoena on the client's behalf. Confirmation will be provided by letter or acknowledged by the attorney on the back of the OIG copy of the subpoena. A copy of the subpoena will also be mailed to the intended recipient with notice of service of the subpoena on the attorney acting for that individual or entity.

230.9 Return of Service. Whenever service of a subpoena is made, proof of such service will be recorded on the “Return of Service” form. (See Appendix C.)

- A. Requirements. The Return of Service will show the particular method by which the subpoena was served (for example, personal service or service by facsimile). The return will also include the date, time, and location of service, and upon whom the subpoena was served. The return of service will also note the serving OIG agent's name and signature.
- B. Service by Mail. If service of a subpoena was accomplished by registered or certified mail (return receipt requested), the completed return receipt will be attached to the return of service section of the duplicate subpoena.

230.10 Modification of Subpoenas. Persons or entities who have received an OIG subpoena may seek to change or modify its terms. Modifications may involve postponements of return dates, changes in the designated location for production of records, substitution of a person producing the records for the person named in the subpoena, or limitations on the number or type of records to be produced. With concurrence of his or her immediate supervisor, an OIG agent may accede to any reasonable request for modification made in apparent good faith, provided it does not impede the OIG inquiry. A description of any modification will be recorded in the appropriate investigative case file, including the identity of the person requesting the modification and the date the change was agreed to.

230.11 Production of Records.

- A. Personal Appearance. The recipient of a subpoena must appear with the records on the specified date and at the specified time and place, even if the recipient intends to refuse to comply with the subpoena. In lieu of personal appearance, the recipient of a subpoena may mail or deliver copies of requested documents together with a signed “Certificate of Compliance,” in accordance with the cover letter that accompanies the subpoena.

- B. Original Documents. The record custodian generally must produce the original records. However, receipt of original records may be dispensed with in connection with third party record holders, such as banks, public utilities, telephone companies, Internet service providers, or airlines. Otherwise, obtain and examine original documents or any copy effectively serving as an original record, such as certified copies or carbon copies of correspondence, invoices, or deposit slips.
- (1) If original documents are sought for initial review, the subpoena cover letter (Appendix A) must be modified. (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
- (2) Upon receipt of original documents, they will be examined and a determination made as to whether copies of the documents will suffice. If any extensive examination of the original record is required and the subpoenaed party shows either a need to access the original records or that the absence will cause a serious business disruption, arrangements will be made with the subpoenaed party for the copying and return of the records pending full examination of the originals. The subpoenaed party bears all copying expenses.
- C. Inventorizing and Safeguarding Subpoenaed Records. To establish a record for administrative and possible evidentiary purposes, the records will be inventoried at the earliest practicable opportunity. Once obtained, the documents will be safeguarded with the same care given to other evidence and regard for chain of custody as set forth in the Inspector General Manual, Volume III, Chapter 234, "Evidence."
- D. Certificate of Compliance. The person producing the records will acknowledge compliance with the subpoena by executing a "Certificate of Compliance." (See Appendix F.) A refusal to sign a Certificate of Compliance or the wholesale "dumping" of unorganized and voluminous documents will constitute a failure to fully comply with the subpoena and will result in court action by the OIG against the subpoenaed party.
- E. Return of Subpoenaed Records. Return the original records to the record custodian and obtain a receipt only after the investigation is completed. A matter is not considered completed until the OIG investigation is closed and all criminal, civil, and administrative actions have ended.
- F. Noncompliance. In the event of noncompliance, the field office will immediately notify and provide OGC with a copy of the executed subpoena, the "Return of Service," and a Memorandum of Investigation summarizing all events surrounding the noncompliance with the subpoena. In conjunction with OGC, the case agent

will prepare an affidavit for use in court to obtain judicial enforcement of the subpoena.

230.12 Privileges Against Disclosure of Records. On occasion, recipients of a subpoena may claim the existence of testimonial privileges that might justify a refusal to disclose records if established. A claim of privilege does not excuse a subpoenaed party from appearing to assert the claim and from identifying the related records. A blanket claim of privilege is unacceptable.

A. Self-Incrimination (Fifth Amendment). The privilege against self-incrimination (Fifth Amendment) protects an individual from being compelled (as by a subpoena) to make disclosures that could be used against him or her in a criminal proceeding. The privilege applies to testimonial disclosures but has been held to apply to a person's compulsory disclosure of incriminating information contained in that person's own records. The courts have held that this privilege is not available in the following situations:

- (1) when records of corporations, unions, organizations, and partnerships are subpoenaed, even if the records happen to incriminate an entity or an individual, the custodian is required to produce them when the act of production, as opposed to the records themselves, is not incriminating to the custodian;
- (2) when records of an individual are subpoenaed from a third party in possession of such material but the individual to whom the records pertain is not actually compelled to produce them (for example, when an individual's records are subpoenaed from an accountant);
- (3) when records of an individual are subpoenaed from another person in custody of the records who may be incriminated by them (for example, when records made by a tax preparer are subpoenaed from the taxpayer);
- (4) when records are required to be kept by law; or
- (5) when records are subpoenaed from a person who has been given immunity.

B. Attorney-Client Privilege. An attorney-client privilege may be invoked to prevent the disclosure of records or communications held by an attorney only if:

- (1) the person claiming the privilege is, or has sought to become, a client of the attorney in question;
- (2) the attorney to whom the communication was made is a member of the bar of a court (or a subordinate of such a member) and is acting, or has acted, as an attorney in connection with the communication or record in question;

- (3) the communication or record in question relates to a fact of which the attorney was informed by the client without the presence of strangers, primarily for the purpose of securing an opinion on law or legal services or assistance in some legal proceeding and not for the purpose of committing a crime or tort; and
- (4) the privilege has been claimed and not waived by the client (this privilege may not be claimed by the attorney).

Even when satisfied, however, the foregoing conditions are not an absolute bar to the enforcement of a subpoena served on an attorney for a client's records. Several courts have held that the attorney can only refuse production of those records that the client would have been able to withhold on the grounds of an independent privilege, usually the self-incrimination privilege.

230.13 Special Procedures Under the Right to Financial Privacy Act of 1978. The Right to Financial Privacy Act of 1978 (RFPA) (12 U.S.C. §§ 3401-3422) applies to subpoenas directed to financial institutions and credit card issuers for production of financial records of their customers. In substance, this statute requires written notice to the customer that his financial records have been subpoenaed and affords the customer an opportunity to challenge the subpoena in court. As discussed below, the government may obtain a court order delaying notice to the customer.

- A. When the RFPA Applies. The RFPA applies only where the records of an individual or a partnership of five or fewer individuals are sought from a financial institution. Financial records of a corporation, a business trust, or a partnership comprised of six or more individuals are not covered by the statute. In addition, the RFPA does not apply if the bank records are sought from a source other than a financial institution; that is, it is permissible to subpoena banking records from an individual or from an accountant without complying with the RFPA.
- B. Obtaining Records With Customer Consent. A customer may voluntarily consent to a review of his or her records. Such consent must be written, limited to three months in duration, revocable by the customer at any time prior to disclosure, and state the purpose for disclosure and the customer's rights under the RFPA. A "Customer Consent" (Appendix J) must be fully executed. The "Customer Consent" is then given to the financial institution and no subpoena is required.
- C. Obtaining Customer Records Without the Customer's Consent.
 - (1) Notice to Financial Institution. If no customer notice is being sought, the first step in the process is service of the subpoena on the financial institution. A "Notice to Financial Institution" (Appendix J) will be delivered with the subpoena. This notice informs the bank that the RFPA applies to the records being subpoenaed.

- (2) Customer Notice. The RFPA requires that the customer be notified, personally or by mail, on or before the date the subpoena is served upon the financial institution. At that time, the customer will be provided with copies of the following:
 - a. a “Customer Notice” letter (Appendix J), specifying the reasons why the financial records are being sought and setting forth the customer's rights under the RFPA;
 - b. a copy of the subpoena (OIG Form III-230/2);
 - c. a copy of the instructions for filing a customer challenge under the RFPA (Appendix J);
 - d. a motion that the customer may complete and file with the court in order to challenge the subpoena (Appendix J); and
 - e. a sworn statement that the customer may complete and file in support of this motion (Appendix J).

- (3) Challenges to an Inspector General Subpoena by the Customer. In order to perfect his or her challenge, the customer must file the motion and sworn statement with the court within 10 days from the date the customer received the subpoena and notice (if by personal service) or within 14 days from the date the notice was mailed.
 - a. Once the applicable time period has expired, the government may proceed to obtain the documents from the financial institution. This is accomplished by delivering or mailing to the financial institution a “Certificate of Compliance” with the RFPA (Appendix J) executed by OGC.
 - b. In the event the customer files a challenge, the customer is instructed to send a copy to OGC. OGC will notify the case agent and coordinate any subpoena enforcement activity with the agent.

- (4) Proceeding After Mailing Customer Notification. Where service of the customer notice is accomplished by mail, the mailing will be both by regular mail and certified mail, return receipt requested, to the customer’s last known address. The agent will wait until 14 days have lapsed before proceeding further.

- (5) Transfer of Records to Another Agency. The RFPA imposes significant restrictions upon interagency transfers of financial records and requires written notice of such transfer to the customer. Any transfer or disclosure

outside DOJ of financial records obtained under the RFPA requires prior consultation with OGC.

- D. Delayed Customer Notification. Where secrecy or surprise is essential to the investigation and can only be achieved if the customer is not notified of the subpoena, the delayed customer notification provisions of the RFPA may be utilized. Under this procedure, the government must go to court before serving a subpoena. If the court finds that prior notice to the customer will seriously jeopardize the investigation or that there is reason to believe that other specified events will occur, the court may issue an order delaying for up to 90 days the customer service of notice by the OIG and also prohibit the financial institution from informing the customer that his or her financial records have been subpoenaed. The 90-day delayed notification may be extended by subsequent applications to the court. An order delaying customer notification must be supported by compelling evidence.
- (1) Basic information can be subpoenaed without implicating the customer notification requirements of the RFPA, including account identifying information limited to the name of the customer, the customer's address, account number, and type of account. (b) (7)(E)
[REDACTED]
 - (2) To obtain specific account records, a second subpoena could be delayed until the knowledge that an investigation is taking place is less sensitive or when the customer's role in the activities under investigation becomes more apparent.

230.14 Reimbursement to Financial Institutions The OIG is required to reimburse financial institutions, at their request, for costs incurred in gathering, reproducing, and delivering financial records pertaining to individuals and small partnerships (six or fewer partners) subpoenaed under the RFPA. Costs incurred in producing account records for corporations, large partnerships, or other legal entities are not reimbursable.

- A. Rates. Reimbursement rates and conditions are set by the Board of Governors of the Federal Reserve System. Additionally, the reasonable cost of transporting the documents to the location called for in the subpoena is reimbursable. Section 3, part 219, title 12 of the Code of Federal Regulations (12 C.F.R. § 219.3) contains updated reimbursement rates.
- B. Payment Process. The OIG agent initiating the subpoena will receive and review the invoice requesting reimbursement. After verifying the accuracy of the invoice as to the actual number of documents provided and that the time spent in producing the documents is reasonable, the agent will forward the invoice to the OIG's Management and Planning Division for payment. The OIG case number and subpoena number will accompany the invoice.

- 230.15 Electronic Communications Privacy Act (ECPA). The stored communication portion of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2712, creates statutory privacy rights for customers and subscribers of computer network service providers and regulates how the government can obtain stored account information from such providers. Whenever OIG agents seek stored e-mail, account records, or subscriber information from a network service provider, they must comply with the ECPA. For additional information regarding the use of OIG subpoenas under ECPA, see the Inspector General Manual, Volume III, Chapter 260, Section 29.
- 230.16 Parallel Proceedings. There is no bar to the simultaneous pursuit of criminal, civil, and administrative remedies if each proceeding is brought in good faith. However, problems involving parallel proceedings and the OIG's subpoena powers can arise in two contexts: the use of administrative process for criminal investigative purposes and the use of the grand jury to elicit evidence for civil or administrative purposes. The misuse in either context is based primarily on due process concerns. Accordingly, the following general rules apply:
- A. Pre-Referral to Prosecutor. An OIG subpoena may be used to further a criminal or administrative investigation prior to determination and reporting to a USAO of a violation of federal law.
 - B. Post Referral to Prosecutor but Pre-Grand Jury. After referral to the prosecutor but before the grand jury stage, an OIG subpoena may be used for any purpose if there is full disclosure between the prosecutor and the OIG. Concurrence in the use of an OIG subpoena from the prosecutor will be sought.
 - C. Post Referral to Grand Jury. Rule 6(e) of the Federal Rules of Criminal Procedure requires secrecy in matters occurring before the grand jury. Information obtained with an OIG subpoena is not subject to the rule 6(e) secrecy requirement. Agents should seek guidance from the USAO or OGC when OIG subpoenas are contemplated while a grand jury investigation is ongoing.

Cover Letter for Field-Issued Subpoenas

(OIG Letterhead)

DATE

Custodian of Records
Company Name
Attn: _____
Street Address
City, State ZIP Code

Dear Name:

The enclosed subpoena duces tecum has been issued under the Inspector General Act, as amended (5 U.S.C. app. 3 § 6(a)(4)). Materials identified in the subpoena should be delivered to:

(Agent Name), Special Agent
U.S. Department of Justice
Office of the Inspector General
Street or Post Office Address
City, State ZIP Code
(Area code) Number

Your personal appearance is required at the time indicated on the subpoena in order to affirm the completeness, accuracy, and authenticity of the documents produced. In lieu of a personal appearance, you may comply with this subpoena by mailing copies of the requested documents together with a signed Certificate of Compliance, which has been provided with this letter. If complying by mail, the documents should be sent to the above address.

Fully legible and complete copies of the records called for by the subpoena will be accepted in response to the subpoena, provided that the original records will be made available for comparison and verification upon request during normal business hours. Otherwise, original documents should be produced.

If any required materials are not furnished, you must list and indicate the location of such materials and the reason for nonproduction.

This investigation is private, and we request such privacy be maintained.
Enclosed is a notice pursuant to the Privacy Act of 1974.

You should bear in mind you have the right to consult with and be represented by an attorney in connection with this matter. If you have any questions concerning the subpoena or the materials required to be produced, please call the Special Agent at the telephone number referenced above.

Sincerely,

Name
Special Agent in Charge

Enclosures

APPENDIX B

IG Subpoena
(OIG Form III-230/2)

No. []

Office of the Inspector General

DEPARTMENT OF JUSTICE

Washington, D.C.

SUBPOENA DUCES TECUM

To: Custodian of Records
Company Name
Attn:
Street Address
City, State ZIP Code

YOU ARE HEREBY COMMANDED TO APPEAR BEFORE

Special Agent (b) (6), (b) (7)(C), an official of the Office of the Inspector General, at 1200 Bayhill Drive, Suite 220, San Bruno, California, on the 12th day of October, 2004, at 9 a.m., in connection with an investigation into allegations of misconduct by an employee of the Department of Justice.

And you are hereby required to bring with you and produce at said time and place all information, documents, reports, answers, records, accounts, papers, and other data and documentary evidence relating as follows:

For the period January 1, 1994, to the present, subscriber information and records of tolls relating to telephone number 1 (800) 500-2558.

which are necessary in the performance of the responsibility of the Inspector General under the Inspector General Act of 1978, as amended, title 5 of the United States Code, app. 3, to conduct and supervise audits and investigations, to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud and abuse in and relating to the programs and operations of the Department of Justice.

IN TESTIMONY WHEREOF, the undersigned,
the Inspector General of the Department of Justice,
or designee, has hereunto set his or her hand on
this _____ day of _____, 20 ____.

PLEASE NOTE: Responsive documents may be mailed to: Special Agent (b) (6), (b) (7)(C), DOJ, Office of the Inspector General, 1200 Bayhill Drive, Suite 220, San Bruno, CA 94066.

APPENDIX C

Return of Service

APPENDIX D

Sample Language for Field-Issued Subpoenas

For the period _____ (dates):

1. Subscriber, tolls, and local usage details for any and all telephone numbers subscribed to by _____ (name), at _____ (address) or any other location, including but not limited to _____ (identified telephone numbers).
2. Any and all services provided to each such number (for example, call waiting and call forwarding) identified in response to Request No. 1.
3. The identity and account number of any additional service providers identified in response to Request No. 1.
4. Any and all charges and identifying information (including date, telephone number called, and minutes) associated with telephone calling card accounts subscribed to by the persons identified in response to Request No. 1.

OR

All customer or subscriber account information for the following e-mail account: (INSERT E-MAIL ADDRESS).

For each such account, the information shall include the subscriber's:

1. Name;
2. Address;
3. Local and long distance telephone toll billing records;
4. Records of session times and durations;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as an Internet Protocol Address; and
7. Means and source of payment for such service (including any credit card or bank account number).

For the period _____ (dates):

1. Any and all charges incurred by customer _____ (name) in the rental of a motor vehicle.
2. Type of vehicles rented and dates rented.
3. Rental car location where vehicle was picked up; rental car location where vehicle was turned in.

OR

For the period _____ (dates):

Any and all records relating to the rental of lodging at _____ (address) by guest _____ (name); records should at least include lodging dates, method of payment, room service, in-room movies, or any other lodging related expenses.

OR

For the period _____ (dates):

Any and all records relating to the provision of electric (or gas, water, and so forth) services to _____ (address), including all identifying information relating to the customer and all billing information for the service address.

OR

For the period _____ (dates):

Any and all records relating to Western Union money orders/wire transfers sent by _____ (name);

OR

For the period _____ (dates):

Any and all records relating to Western Union money orders/wire transfers received by _____ (name);

OR

For the period _____ (dates):

Any and all records relating to Western Union money orders/wire transfers [sent by] OR [received by] _____ (name) originating [in] or [from] _____ (geographic area).

Privacy Act Notice

Notice Pursuant to Privacy Act of 1974

The Privacy Act of 1974 directs that persons, such as those required by the Inspector General of the Department of Justice (DOJ) to supply information in response to a subpoena, be informed of the following:

1. Authority for Solicitation of the Information:

The authority for requiring production of the information is set forth in the Inspector General Act of 1978, as amended by the Inspector General Act Amendments of 1988, 5 U.S.C. app. 3, 6(a)(4). Disclosure of the requested information is mandatory.

2. Principal Uses of the Information:

The Inspector General's principal purpose in soliciting the information is to promote economy, efficiency, and effectiveness in the administration of the programs and operations of DOJ and to prevent and detect fraud and abuse in such programs and operations.

3. Effect of Noncompliance:

Failure to comply with a subpoena may result in the Inspector General requesting a court order for compliance. If such an order is obtained and you thereafter fail to supply the information, you may be subject to civil and/or criminal sanctions for contempt of court.

4. Routine Uses of the Information:

Information you give may be used and disseminated in the routine operation of DOJ, including criminal, civil, and administrative proceedings. Routine uses include, but are not limited to, the following categories:

- (a) In any case in which there is an indication of a violation or a potential violation of law, whether civil, criminal, or regulatory in nature, the record in question may be disseminated to the appropriate federal, state, local, or foreign agency charged with the responsibility for investigating or prosecuting such violation or charged with enforcing or implementing such law;
- (b) In the course of investigating the potential or actual violation of any law, whether civil, criminal, or regulatory in nature, or during the course of a trial or hearing or the preparation for a trial or hearing for such violation, a record may be disseminated to a federal, state, local, or foreign agency, or to an individual organization, if there is reason to believe that such agency, individual, or organization possesses information relating to the investigation, trial, or hearing and the dissemination is reasonably necessary to elicit such information or to obtain the cooperation of a witness or an informant;
- (c) A record relating to a case or matter may be disseminated in an appropriate federal, state, local, or foreign court or grand jury proceeding in accordance with established constitutional, substantive, or procedural law or practices;

- (d) A record relating to a case or matter may be disseminated to an actual or potential party or his attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, plea bargaining, or informal discovery proceedings;
- (e) A record relating to a case or matter that has been referred by an agency for investigation, prosecution, or enforcement, or that involves a case or matter within the jurisdiction of an agency, may be disseminated to such agency to notify the agency of the status of the case or matter or of any decision or determination that has been made, or to make such other inquiries and reports as are necessary during the processing of the case or matter;
- (f) A record relating to a case or matter may be disseminated to a foreign country pursuant to an international treaty or convention entered into and ratified by the United States or to an executive agreement;
- (g) A record may be disseminated to a federal, state, local, foreign, or international law enforcement agency to assist in the general crime prevention and detection efforts of the recipient agency or to provide investigative leads to such agency;
- (h) A record may be disseminated to a federal agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the award or administration of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information relates to the requesting agency's decision on the matter;
- (i) A record may be disseminated to the public, news media, trade associations, or organized groups, when the purpose of the dissemination is educational or informational, such as descriptions of crime trends or distinctive or unique modus operandi, provided that the record does not contain any information identifiable to a specific individual other than information such as a modus operandi.

5. Freedom of Information Act:

The Freedom of Information Act, 5 U.S.C. 552, and the Department's rules pursuant thereto generally provide for access by members of the public to governmental records, unless the requested documents fall within specified exemptions.

APPENDIX F

Certificate of Compliance

CERTIFICATE OF COMPLIANCE

I am responsible for the review of records to identify those covered by the Department of Justice Inspector General Subpoena No. FY- ____ - ____ - ____ , dated ____ . All records in the possession, custody, and control of the person or business to which the subpoena is directed that are covered by the subpoena have been produced and given to a representative of the Inspector General, and, if copies were given instead of the originals, all such documents were accurately and completely copied. No documents have been withheld except those that have been identified to the Inspector General's representative, who has also been given an explanation of the reason why they were not produced.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on _____ , _____.

(Signature)

(Title)

APPENDIX G

Request Form and Checklist for Field-Issued Subpoenas

Case No. _____

Subpoena No. _____

1. How is the investigation within the OIG's jurisdiction?
2. Is the material sought relevant to the investigation?
3. Are sought records identified with sufficient specificity?
4. Is the timeframe for material relevant to investigation?
5. Can the addressee appropriately challenge the request as burdensome?
6. Describe how these records will aid this investigation.

Approve

Disapprove

Special Agent in Charge

Date _____

Field Office

CHECKLIST FOR SUBPOENA PACKAGE

Subpoena No.

Letter to Communications Carrier _____(initials)

Subpoena _____

Attachment to Subpoena
(If applicable) _____

Privacy Act Statement _____

Certificate of Compliance _____

SAC Approval Form _____

(This checklist is only for internal purposes and must not be provided to the addressee.)

APPENDIX H

Field Office Subpoena Log

APPENDIX I

**Example of an Application for Subpoena Requested
Through the Office of General Counsel**

U.S. Department of Justice
Office of the Inspector General

REQUEST FOR ISSUANCE OF AN OIG SUBPOENA

Person delivered to:

Name: (b) (6), (b) (7)(C)
Special Agent

Address: Department of Justice
Office of the Inspector General
60 Forsyth Street, S.W., Suite 8M45
Atlanta, GA 30303

Telephone: (404) 562-1980 Office
(404) 562-1960 FAX

Person to be Served:

Custodian of Records
Money Order Branch
U.S. Postal Service
1720 Market Street, Room 3131
St. Louis, MO 63180-9450

Date Documents
To Be Produced: 30 days from issuance of subpoena.

Time of Appointment: 12 noon

Description of investigation:

On November 9, 2000, the Atlanta Area Office opened investigation (b) (7)(C), (b) (6) concerning allegations that Correctional Officer XXXXX is introducing contraband into the Federal Correctional Institution, Yazoo City, MS, for a fee. XXXXX is providing the contraband to federal inmate XXXXX. Inmate XXXXX agreed to cooperate in this investigation, and an undercover operation was initiated. The OIG sent several packages to XXXXX at his P.O. Box address in MS. The packages were purportedly coming from inmate XXXXX cousin (OIG undercover agent). The packages contained soft contraband and payment for XXXXX for delivering the items to inmate XXXXX. The payment was provided utilizing U.S. Postal money orders. XXXXX delivered the soft contraband to inmate XXXXX, and he negotiated the U.S. Postal money orders.

Description of the documents to be obtained by the subpoena:

The original U.S. Postal Service money orders with the following serial numbers:

- 1) 02712262498 dated 2/21/2001
- 2) 02342342733 dated 12/14/2000
- 3) 02342333665 dated 11/17/2000
- 4) 02506259621 dated 10/06/2000
- 5) 02506259632 dated 10/06/2000

Description of sensitive matters:

There are no sensitive issues concerning the issuance of this subpoena.

Justification for subpoena:

Receipt of the requested materials will determine if XXXXX endorsed the money orders. This information will be used as evidence against XXXXX to prove bribery charges against him.

Steps taken to obtain documents informally and to minimize burden:

Inspector (b) (6), (b) (7)(C), U.S. Postal Inspection Service, Atlanta, GA, advised SA (b) (6) by telephone that the requested information could not be released without a subpoena since the USPIS is not working the case with the OIG.

Does Right to Financial Privacy Act apply?

No.

**Examples of Additional Subpoena Documents
to be Completed by OGC**

Letter to person being subpoenaed

Customer Consent and Authorization for Access

Customer Notice Letter

Instructions for Filing a Challenge under RFPA
- Customer Motion to Challenge under RFPA
**- Customer Sworn Statement to Challenge
under RFPA**

Certificate of Compliance with RFPA

Notice to Financial Institution

EXAMPLE
Letter to Person Subpoenaed

(Address of person subpoenaed)

Dear (name of person subpoenaed)

The enclosed subpoena duces tecum has been issued pursuant to the Inspector General Act, as amended, 5 U.S.C. app. 3 § 6(a)(4). When produced, the materials identified in the subpoena should be delivered to:

(Add address per subpoena)
Office of the Inspector General
Department of Justice

Your personal appearance is required at the time indicated on the subpoena in order to affirm the completeness, accuracy and authenticity of the documents produced. In lieu of a personal appearance, you may comply with this subpoena by mailing copies of the requested documents together with a signed Certificate of Compliance, which has been provided with this letter. In such case, the documents should be mailed to the above address.

Fully legible and complete copies of the records called for by the subpoena will be accepted in response to the subpoena provided that the original records will be made available for comparison and verification, upon request, during normal business hours. Otherwise, original documents should be produced.

If for any reason any of the required materials are not furnished, you must list and indicate the location of such materials and the reason for nonproduction.

This investigation is private, and we request such privacy be maintained.
Enclosed herewith is a notice pursuant to the Privacy Act of 1974.

You should bear in mind you have the right to consult with and be represented by an attorney in connection with this matter. If you have any questions concerning the subpoena or the materials required to be produced, please call the Special Agent at the telephone number referenced above..

Sincerely,

Special Agent in Charge

Enclosures

EXAMPLE

**CUSTOMER CONSENT AND AUTHORIZATION
FOR ACCESS TO FINANCIAL RECORDS**

I, _____ having read the explanation of my rights which is attached to
(Name of Customer)

this form, hereby authorize the _____
(Name and address of Financial Institution)

to disclose these financial records (describe):

to the Office of the Inspector General, Department of Justice, for the following purpose(s):

I understand that this authorization may be revoked by me in writing at any time before my records, as described above, are disclosed, and that this authorization is valid for no more than three months from the date of my signature.

_____, 20__
(Date)

Signature of Customer

(Address of Customer)

EXAMPLE
Customer Notice Letter

CUSTOMER NOTICE

[Name and address of customer]

Dear _____:
(Customer Name)

Records or information concerning your transactions held by the financial institution named in the attached subpoena are being sought by the Department of Justice Office of the Inspector General (OIG) in accordance with the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 - 3422 for the following purpose:

If you desire that such records and information not be made available, you must:

- (1) Fill out the accompanying motion paper and sworn statement (as indicated by the instructions beneath each blank space) or write one of your own, stating that you are the customer whose records are being requested by the OIG and giving either the reasons you believe that the records are not relevant to the legitimate law enforcement inquiry stated in this notice or any other legal basis for objecting to the release of the records.
- (2) File the motion and sworn statement by mailing or delivering them to the Clerk of either of the following United States District Courts:

It would assist the proceeding if you would include with your motion and statement a copy of the attached subpoena(s), as well as a copy of this notice.

- (3) Serve the OIG by mailing (registered or certified mail is suggested) or by delivering a copy of your motion and sworn statement to:

General Counsel
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, NW., Room 4726
Washington, D.C. 20530

- (4) Be prepared to come to court and present your position in further detail.
- (5) You do not need to have a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of ten days from the date of service or fourteen days from the date this notice is mailed, the records or information requested therein may be made available to the OIG. These records may be transferred to other government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer.

Sincerely,

General Counsel

Enclosures: Subpoena
Instructions for Filing Challenge
Motion Form
Sworn Statement Form

EXAMPLE
Instructions

INSTRUCTIONS FOR COMPLETING AND FILING THE ATTACHED
MOTION AND SWORN STATEMENT

1. Except where signatures are required, the indicated information should be either typed or printed legibly in ink in the spaces provided on the attached motion and sworn statement forms. The information required for each space is described in parentheses under each space to be completed.
2. The most important part of your challenge application is the space on the “sworn statement” form where you must state your reasons for believing that the financial records sought are not relevant to the legitimate law enforcement inquiry stated in the attached notice. You may also challenge the Government's access to the financial records if there has not been substantial compliance with the Right to Financial Privacy Act or for any other reasons allowed under the law. You should state the facts that are the basis for your challenge as specifically as you can.
3. To file your challenge with the Court, either mail or deliver the original and one copy of your challenge papers to the Clerk of the United States District Court you choose to have decide the case (you may select the court of the district in which you reside, the court where the documents are located (which may be the same), or the District of Columbia). You should call the Clerk of the court to determine the amount of the court's filing fee and what methods of payment are accepted.
4. One copy of your challenge papers (motion and sworn statement) must be delivered or mailed (preferably by registered or certified mail) to the official of the Office of the Inspector General who signed the accompanying letter at his or her office address.
5. If you have further questions, contact the Government official whose name and telephone number appear on the Customer Notice.

CERTIFICATE OF SERVICE

I have mailed or delivered a copy of this motion and the attached sworn statement to

(Name of Official Listed at Item 3 of Customer Notice)

on _____, ____, 20____.
(Date)

(Your Signature)

Section 1110 of the Right to Financial Privacy
Act of 1978, 12 U.S.C. § 3410

CUSTOMER'S SWORN STATEMENT
FOR FILING A CHALLENGE

IN THE UNITED STATES DISTRICT COURT

FOR THE _____ DISTRICT OF _____
(Name of District) (State in Which Court Is Located)

_____) Miscellaneous No. _____
(Customer's Name))
(Will Be Filled in by Court
Movant) Clerk)
)

v.)

Department of Justice) SWORN STATEMENT OF MOVANT
)
Respondent.)

I, _____, (am presently/was previously)
(Customer's Name) (Indicate One)

a customer _____,
(Name of Financial Institution)

and I am the customer whose records are being requested by the Government.

The financial records sought by the Office of the Inspector, U.S. Department of Justice, are not relevant to the legitimate law enforcement inquiry stated in the Customer Service Notice that was sent to me because

or should not be disclosed because there has not been substantial compliance with the Right to Financial Privacy Act of 1978 in that

or should not be disclosed on the following other legal basis

I declare under penalty of perjury that the foregoing is true and correct.

_____, 20____
(Date) (Customer's Signature)

EXAMPLE
Certificate of Compliance With RFPA

(OIG Letterhead)

DATE

NAME AND ADDRESS OF FINANCIAL INSTITUTION

Re: U.S. Department of Justice
Office of the Inspector General Subpoena No. XXX

Dear Sir or Madam:

In accordance with the Right to Financial Privacy Act (the Act), 12 U.S.C. § 3403(b), I hereby certify that the Office of the Inspector General (OIG) has complied with the applicable provisions of the Act with regard to OIG Subpoena No. XXX, dated XXX, which seeks the following records:

(INSERT FROM SUBPOENA OR NOTICE
TO FINANCIAL INSTITUTION, AS APPLICABLE)

Pursuant to the Act, good faith reliance upon this certification relieves your institution and its employees and agents of any liability to the customer in connection with the disclosure of these financial records. 12 U.S.C. § 3417(c). Accordingly, please provide the requested records to Special Agent XXX in accordance with the instructions that were previously provided to you.

Sincerely,

Gail A. Robinson
General Counsel

EXAMPLE
Notice to Financial Institution

NOTICE TO FINANCIAL INSTITUTION

The subpoena just delivered to you was issued by the Inspector General of the United States Department of Justice pursuant to the Inspector General Act of 1978, 5 U.S.C. § 6(a)(4). The subpoena seeks records that may be covered by the Right to Financial Privacy Act of 1978 (RFPA), 12 U.S.C. § 3401. Accordingly, this office has notified your customer of the existence of the subpoena and of the rights available to him or her under the Act. You should not provide documents in response to the subpoena until you have receive notification to do so from this office.

In the meantime, we ask that you begin the search and retrieval of the records sought by the subpoena. Under the RFPA, 12 U.S.C. § 3415, and the regulations implementing that provision, 12 C.F.R § 219.3, you are entitled to request reimbursement for the costs directly incurred and reasonably necessary in producing the documents, at the rate of \$11 per hour for clerical or technical personnel and \$17 per hour for manager or supervisory personnel for searching and processing costs, and 25 cents per page for reproduction costs. These costs are reimbursable for search work done now, even should the subpoena be challenged and disallowed by a court. Accordingly, we ask that you begin immediate work on production of the records. If, however, you estimate that the total costs incurred in responding to this request will exceed \$250.00, you should notify the Special Agent identified on the subpoena before going further with the search. Finally, your bill for the costs of producing these records must itemize and provide specific details concerning the costs incurred, the identity of employees assigned directly to the search, and the amount of time each spent on it.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 230
Subpoenas
Revisions

This chapter was previously revised on June 10, 2009, and April 23, 2007, and originally issued on July 7, 1995. This chapter was rewritten to reflect updates and changes in policies, laws, and guidelines.

Changes issued in this revision, dated January 2, 2014, are in the following sections:

- 230.5:** Changes field-issued subpoenas to INV-issued subpoenas. Adds authority to issue INV-issued subpoenas to all SACs and the Chief, Digital Forensics and Technology Investigations Unit. Clarifies that the AIG and the DAIG have authority to issue subpoenas.
- 230.5D:** Adds guidance regarding telephone and Internet subscriber information requiring OGC review (in accordance with guidance issued in e-mail policy clarification on February 23, 2012).
- 230.6:** Deletes reference to IDMS blank forms availability.
- 230.6B:** Refers user to the OIG Intranet Investigations Division home page for IGM Form III-230/2 for field-issued subpoena for telephone and Internet subscriber information and to Appendix B for field-issued customizable IGM Form III-230/2 (in accordance with guidance issued in e-mail policy clarification on February 23, 2012).
- 230.6H:** Adds example of subpoena numbering for the DFTIU.
- Appendixes C, E, and F:** Updated to show OIG Intranet Investigations Division home page IGM Form III-230/2 documents.

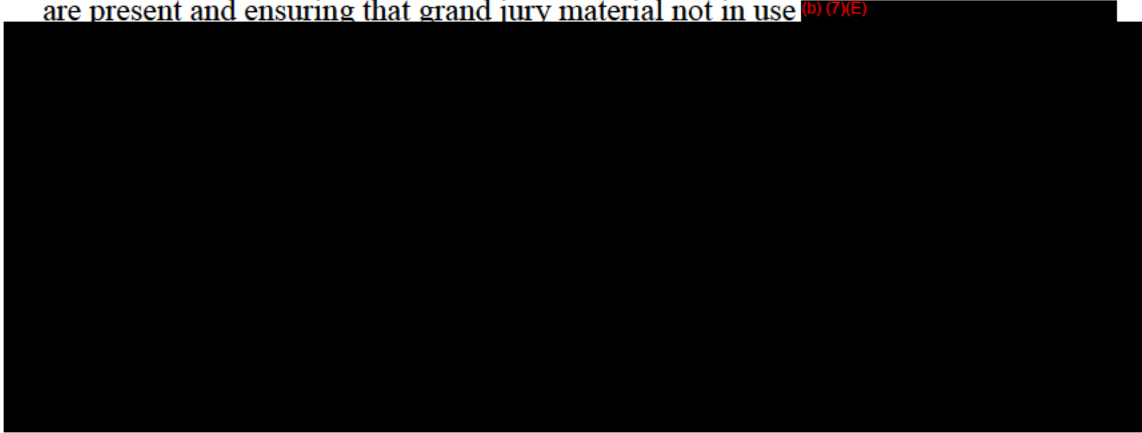
Changes, additions, and deletions in guidance issued on June 10, 2009, appear in the following sections:

- 230.5:** Adds guidance regarding Federal Bureau of Prisons investigations and authority to issue subpoenas for money order information.
- 230.7:** Changes paragraph title to state “OGC-Issued Subpoenas,” rather than “Headquarter Issued Subpoenas.”
- 230.7D:** Adds guidance regarding OGC-issued subpoenas for subscriber information from telephone and Internet service providers
- 230.14:** Deletes reference to specific reimbursement rates, as these are subject to change by the Board of Governors of the Federal Reserve System.

Throughout appendixes, updates sample documents.

- 231.1 Policy. This chapter establishes Office of Inspector General (OIG) policy and procedures for handling and safeguarding information obtained through the grand jury process and federal income tax and medical information pertaining to individuals. Personnel of the OIG must protect sensitive unclassified information originating from federal grand jury proceedings, an individual’s federal tax return, and personal medical records from unauthorized disclosure.
- 231.2 Reference. This chapter is issued pursuant to the authority contained in the Inspector General Act of 1978, appendix of title 5 of the United States Code (5 U.S.C. app), as amended; Federal Rules of Criminal Procedure, Rule 6(e); Department of Justice Order 2600.4, dated August 27, 1980, “Safeguarding Grand Jury Information”; 26 U.S.C. § 6103, et. seq., “Internal Revenue Code, section 6103 - Confidentiality of Returns and Return Information”; the Health Insurance Portability and Accountability Act of 1996 (Public Law (Pub. L.) 104-191); and parts 160 and 164, title 45, Code of Federal Regulations (45 C.F.R. §§ 160, 164), protected health information.
- 231.3 Scope. The provisions of this chapter apply to all employees in the OIG Investigations Division (INV).
- 231.4 Grand Jury Materials.
- A. Limitations on Use. Rule 6(e) of the Federal Rules of Criminal Procedure provides in part that any person to whom grand jury matters are properly disclosed:
- “...shall not utilize that grand jury material for any purpose other than assisting the attorney for the Government in the performance of such attorney’s duty to enforce Federal criminal law.”
- (1) Generally, information or evidence obtained through the federal grand jury process may not be used in administrative, disciplinary, or other non-criminal proceedings. OIG special agents should consider this limitation when deciding whether to seek information via grand jury or OIG (administrative) subpoena.
- (2) Any expanded use of grand jury information requires a court order that is based on a motion filed by the U.S. Attorney’s Office.
- B. Limitations on Access. Only OIG employees in receipt of a Rule 6(e) letter from the United States Attorney (U.S. Attorney) shall have access to grand jury information. In most circumstances, the cognizant Assistant U.S. Attorney shall be advised that, in addition to the investigating agents assigned to a matter that is before a grand jury, the investigating agent’s assistant special agent in charge and special agent in charge, as well as the Deputy Assistant Inspector General for Investigations and Assistant Inspector General for Investigations, should be included among those authorized access to the grand jury information. In some

cases, other individuals, such as clerical support personnel, auditors, the evidence custodian, certain Investigations Division Headquarters personnel, the General Counsel and other OIG Counsel, the Deputy Inspector General, or the Inspector General, may also need to be designated for access to grand jury material.

- C. Safeguarding Grand Jury Material. Whenever grand jury information is obtained, the responsible agent shall ensure that it is safeguarded at all times from improper disclosure and shall consult with the prosecutor on proper custody and maintenance of the records. This may require keeping direct physical control over the material, ensuring that material in use is protected when persons without authorized access are present and ensuring that grand jury material not in use (b) (7)(E)
- 

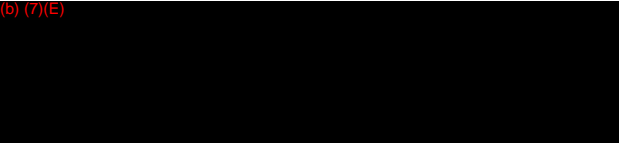
- (2) All grand jury information will be returned to the responsible prosecutor upon termination of the investigation. However, if requested by the prosecutor, such material may be destroyed by OIG personnel or returned to the supplier/originator. In any case, the ultimate method of disposal will be cleared through the prosecutor. The investigative case file shall note the authorizing official and the method used to dispose of grand jury information

231.5 Federal Tax Information.

- A. Limitations on Access and Use. The OIG may obtain tax returns and taxpayer return information directly from the taxpayer (either voluntarily or pursuant to an Inspector General subpoena), from third party sources such as accountants, or pursuant to a joint investigation where the information is in the custody of the other investigating agency. However, such information may not be obtained from the Internal Revenue Service (IRS) except under very limited circumstances. Specifically, section 6103 of the Internal Revenue Code (IRC) (26 U.S.C.) provides that tax returns and return information may be obtained from the IRS only pursuant to a court order and only in connection with the investigation of a federal crime. The application to the court must be approved by the Attorney General, Deputy Attorney General, an Assistant Attorney General, a U.S. Attorney, or an attorney in charge of an organized crime task force.

Regardless, of how the tax information is obtained, agencies are required to restrict access to the information to those persons whose official duties and responsibilities require access. Within the OIG, this is typically limited to the investigating agents, auditors, and their supervisors. Unauthorized disclosure of tax information can subject an individual to significant criminal and civil penalties.

For purposes of this chapter, protected federal tax information (FTI) consists of returns and return information contained in or derived directly from the federal income tax filings of individuals. FTI relating to corporations or partnerships is generally excluded from protection under the IRC. The term return means any tax or information return, declaration of estimated tax, or claim for refund required by or provided under the provisions of the IRC. The term return information means a taxpayer's identity; the nature, source, or amount of his or her income; payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, over assessments, tax payments, or other data furnished to or derived directly from information collected by the IRS with respect to a tax return or other official function.

- B. Safeguarding Federal Tax Information. In order to avoid inadvertent disclosure, FTI shall be kept separate, to the extent possible, from other case-related information and filed and stored ^{(b) (7)(E)} 

Similarly, FTI shall not be commingled with other data on electronic computer media. Any electronic media containing FTI must be safeguarded in the same manner as hard copy or paper files containing FTI. Computer systems used to process FTI should be access protected, and FTI shall not be placed in the text of electronic mail traffic but attached and encrypted.

- (1) Although IRC section 6103 generally prohibits the disclosure of FTI in possession of the OIG to other government agencies, there are certain exceptions authorizing its release. The determination as to whether tax information can be disclosed is fact specific, and before any disclosure, the federal prosecutor who is involved with the investigation or the OIG Office of General Counsel should be consulted.
- (2) Once FTI is no longer being used (once the case is closed), agents must ensure that FTI is destroyed or returned to the originating agency or person, including any copies. If the FTI is not physically destroyed by OIG personnel through shredding or burning, the destruction of FTI by a contractor storing OIG records shall be witnessed by OIG personnel. Alternatively, the destruction may be certified by the contractor if the contractor meets the required standard safeguard provisions of 26 C.F.R. § 301.6103(n)-1.

231.6 Protected Health Care Information.

- A. Limitations on Access and Use. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) generally prohibits disclosure of individually identifiable health information (personal medical records). 45 C.F.R. § 164 provides limited exceptions allowing disclosure of individual medical records for certain purposes, such as a legitimate law enforcement inquiry by subpoena or court ordered warrant or with consent of the individual to whom the records pertain. However, 45 C.F.R. § 164 also requires that disclosure be limited only to that information that is needed to carry out authorized functions and further requires that such medical records be safeguarded and protected from additional disclosure except as specifically authorized in the C.F.R.
- B. Safeguarding Medical Records. Individual medical records pertaining to a victim, witness, or subject of an OIG investigation must be protected from unauthorized disclosure and may be shared only with other personnel who have a need to know, such as the case agent’s supervisor, the prosecutor handling the case, or agents assisting in the investigation. When not in use, such records should be stored separately from the relating case file in a locked storage container. If this is not practicable, then the outside of the investigative case folder must be clearly marked that it contains “individual health information” as defined in HIPAA.
- (1) Personal medical information stored in electronic media may not be commingled with other data or information and should be safeguarded in the same manner as paper records.
 - (2) Before the case is closed, personal medical information should be destroyed or returned to the originator. Destruction must be by burning or shredding. If destruction is carried out by an OIG contractor, the destruction must be witnessed by OIG personnel, or the destruction may be certified by the contractor if the contractor meets the required standards for safeguarding protected medical information.

231.7 Reporting Requirements. The appropriate OIG security officer shall be notified in writing in any of the following situations:

- A. A threatened, attempted, or actual unauthorized entry into a facility where grand jury work is in process or where grand jury, FTI, or individual health care information is stored.
- B. A suspected or actual loss or compromise of grand jury, FTI, or individual health care information.

- C. A change of contract ownership, operating name, or contract facility address of any OIG records storage contractor or a change in the storage capability that would affect the protection of information that the contractor is required to safeguard.

231.8 Protection Standards for National Security Information. Grand jury, FTI, or health care information that is also classified information must be safeguarded in accordance with the provisions of the Inspector General Manual, Volume I, Chapter 220. Any questions regarding these requirements should be addressed through the security officer, OIG Management and Planning Division.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 231
Grand Jury
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This chapter was originally issued on 10/22/90 and was re-written to reflect updates and/or changes in policies, laws, and/or guidelines.

- 234.1 Policy. This chapter establishes policies and procedures for processing physical evidence seized or otherwise obtained during investigations conducted by the Office of the Inspector General (OIG).
- 234.2 Reference. This chapter is issued pursuant to the authority contained in the Inspector General Act of 1978, Title 5 Appendix, United States Code (U.S.C.), as amended, and the Homeland Security Act of 2002 (Pub. L. No. 107-296).
- 234.3 Scope. Provisions of this chapter apply to all employees in the OIG Investigations Division (INV).
- 234.4 General Evidence Considerations.
- A. An investigation is essentially the process of gathering information and supporting materials. These supporting materials (evidence) are often presented to a fact-finder, along with information in the form of testimony, to prove or disprove that a certain act occurred.
 - B. In order to be admissible as evidence in court or other official proceedings, the gathered materials (which may consist of such things as weapons, narcotics, altered or forged documents, audio- or videotapes, business records, or other items) must be shown to have been in the continuous custody of the government since seizure and not to have been altered or substituted while in the government's possession. To demonstrate this, it is imperative that a proper chain of custody be documented for the materials from the time of collection to the time of ultimate disposition and that, during this time, proper security measures have been followed to preclude tampering with the materials.
- 234.5 Evidence Responsibilities.
- A. Agency Responsibilities. The OIG has both the obligation and responsibility to ensure the accountability and integrity of evidence in the agency's custody. It is incumbent upon the OIG to ensure that all evidence collected is positively identified, strictly accounted for, and properly safeguarded.
 - B. Individual Responsibilities. All OIG personnel who handle evidence must know and follow the agency-mandated evidence collection, marking, storage, and disposal procedures as set forth in this chapter. Personnel must properly identify and account for all evidence upon receipt in order to preclude admissibility issues in any subsequent court proceedings. All OIG Special Agents must properly complete evidence forms and promptly turn in all evidence to the designated OIG evidence custodian for safekeeping.

234.6 Evidence Custodians.

- A. Appointment and Oversight. Each field office Special Agent in Charge (SAC) shall appoint in writing a primary and an alternate evidence custodian. A probationary employee with less than 1 year of Department of Justice (DOJ) OIG experience will not be appointed as the primary evidence custodian but may serve as the alternate evidence custodian.

The names of the primary and alternate evidence custodians will be forwarded to the SAC, Investigative Support Branch, INV Headquarters. All field office SACs must ensure that evidence custodians properly handle and safeguard evidence in their custody.

- B. Duties and Responsibilities. Primary and alternate evidence custodians perform all duties interchangeably. Either custodian may accept evidence, record evidence in the evidence log, and secure evidence in the designated evidence facility. There is no need to transfer evidence between the two custodians. However, the primary evidence custodian is accountable for all evidence in field office custody and is responsible for the oversight of evidence collection activities. The primary and alternate evidence custodians will:
- (1) maintain a secure and orderly evidence facility. Only evidence custodians have unescorted access to the evidence facility;
 - (2) receive evidence for storage, ensure that all evidence is properly marked for identification, and ensure that the accompanying evidence form is accurately completed;
 - (3) maintain the office evidence log to account for all evidence in custody by properly recording the receipt, transfer, and disposition of each item of evidence. Only evidence custodians may make entries in the evidence log;
 - (4) provide guidance and periodic training for office personnel on evidence handling procedures and documentation;
 - (5) perform required periodic evidence inventories; and
 - (6) monitor evidence in custody to ensure prompt disposal following final adjudication of the relating case.

234.7 Evidence Holding Facility Security.

- A. Physical Security. Store all physical evidence in a well-secured room, safe, or other appropriate container. Evidence facilities must be secured as much as practical to prevent theft or surreptitious entry. (b) (7)(E)

(b) (7)(E)

The goal for secure evidence facilities and containers is the safeguarding of evidence against tampering or theft by deterring unauthorized or surreptitious entry.

(b) (7)(E)

B. Access Control. (b) (7)(E)

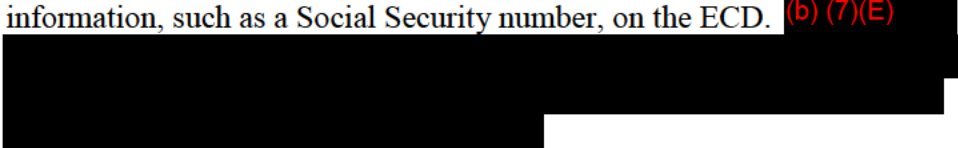
Except for inspections and other required functions, do not allow non-DOJ OIG personnel access to evidence storage facilities or identify such facilities to them.

C. Storage of OIG Weapons in Evidence Facilities. OIG weapons or ammunition may not be stored in the evidence room or evidence vault. (b) (7)(E)

234.8 Evidence Accountability Procedures.

- A. Seizing Evidence — General Procedures. When an item of evidence is originally collected or seized during investigative activity, agents will immediately mark the item with their initials and date. If possible, another agent or law enforcement officer will witness the collecting or seizing of all items of evidence. If possible, place the item in a plastic bag or similar container and attach an evidence label that contains the case number, date of seizure, exhibit number, where the item was found, and the investigator's initials. When evidence is placed in a container, the seal of the container must have an evidence seal affixed to it. The evidence seal will contain the case number, date that the item was sealed, the criminal offense, the location where the item was sealed, and the investigator's initials. All items of evidence must be turned over to the evidence custodian as soon as possible, usually within 24 hours. The seizing agent will complete an OIG Form III-234/1 (Evidence Custody Document (ECD)), documenting the seizure (Appendix A). Upon completing the ECD, the case agent will maintain a photocopy of the ECD in the case file. It is important to note that the ECD is maintained to establish chain of custody and on occasion may itself be the subject of examination during a court proceeding.

B. Evidence Custody Document. The ECD is a single page form designed to record the identity and chain of custody of evidence. It is imperative that all staff properly complete the ECD, as it is the primary record of evidence custody from the time the evidence is seized until its final disposition. When an item of evidence is transferred outside of an OIG storage facility for analysis, the original ECD will accompany the evidence in order to continually track the evidence chain of custody. The evidence custodian will make and maintain a photocopy of the ECD, which will remain in a folder in the evidence room. Prior to closing a case that involves evidence, the case agent will check with the assigned prosecutor to obtain authorization to dispose of the evidence. Accordingly, once authorization is granted to dispose of the evidence, the case agent will inform the evidence custodian of the decision to dispose of the evidence. The evidence custodian will then complete the chain of custody section, signing the evidence out to the case agent and annotating in the purpose block that the evidence is being released to the case agent for final disposition. Within 72 hours after receiving the evidence from the evidence custodian for final disposition, the case agent will dispose of the evidence by documenting the disposition on an OIG Form III 234/4 (Evidence Disposition Document (EDD)). The EDD is a single-page form used to record the final disposition of evidence. Samples of the ECD and EDD are at Appendix A. The following guidelines apply to completion of the ECD and EDD:

- (1) Type or write in all applicable blocks on the ECD. If the ECD is handwritten, agents will use a ballpoint pen or similar hard-tip pen. The evidence custodian will fill in the "Log #" block. Do not enter personal information, such as a Social Security number, on the ECD. (b) (7)(E)

- (2) When completing the "Description of the Property Seized" block on the ECD, remember that the primary purpose is to enable the agent to positively identify the specific item of evidence at a later date. The description should be precise and focus on any unique characteristics or markings that distinguish that item of evidence from other similar items. Refer to alleged gold or silver jewelry or other items as gold-colored or silver-colored and refrain from assigning any monetary value to items of evidence. However, if available, include the owner's estimate of value for private property seized as evidence. If property is to be returned, note its condition, including any significant damage or unusual wear and tear. In instances where there is considerable wear and tear or damage or where the owner's valuation appears to be grossly inflated, the seizing agent should photograph the evidence. Those photographs should be maintained in an envelope in the case file.

- (3) Generally, each item of evidence must be listed on a separate ECD. However, up to three similar items seized from the same location at the same time can be listed on one ECD if each item can be clearly identified at a later date. If an agent seizes a large number of documents/files, each individual document does not have to be listed separately on the ECD but can be identified by groupings, places found, numbers, and dates. A more detailed inventory of the seized documents/files can be completed and recorded on a Memorandum of Investigation (MOI), which will be prepared anytime evidence is obtained. Likewise, if specific documents/files are later identified as items to be used in court, separate ECDs can be filled out.

Before releasing any evidence seized in a bundle or multiple-item seizure, the case agent will compile a complete inventory of that group and document the results on a separate MOI. In addition, for seizures such as bundles of cash, a separate sheet of paper (continuation sheet) specifically listing the serial numbers by denomination or the use of a continuation ECD is authorized.

- (4) The evidence log number will be assigned by the evidence custodian at the respective field office. The evidence log, which is maintained by the evidence custodian, will identify each item of evidence according to the OIG case number and the sequential number (for example, 1, 2, 3). Evidence logs are more fully described in paragraph C below.
- (5) Every time an item of evidence changes custody, enter custody information in the chain of custody section of the ECD. When sending evidence to a laboratory for examination, record "mail transfer" and the U.S. Postal Service (USPS) or other registration number in the "Purpose" block. The original ECD will accompany the item of evidence and a copy will remain with the evidence custodian and the case file. When evidence is returned via USPS (or another carrier) after examination, enter the USPS (or other carrier) registration number in the "Purpose" block.

In addition, check all items of evidence received or released to ensure that the quantity and condition correspond with the description on the ECD and evidence label. The final disposition will be documented in the "Purpose" block of the ECD (for example, "returned to the case agent for destruction"). The final disposition will also be documented on the EDD. When destroying evidence, such as drugs, the individual conducting the destruction will sign both the "Received by" on the ECD and the "Destroyed the Evidence" block on the EDD. Regardless of the circumstances, final disposition will be clearly documented on the ECD. The ECD and the EDD become part of the closed case file and are stored with the file.

- (6) For instances where a receipt is required to obtain items from an individual or company, agents will use OIG Form III-233/2 (Receipt for Cash and Other Items). The ECD will not be used as a receipt to obtain items.
- C. Evidence Logs. Each field and area office holding evidence will maintain an evidence log. The OIG evidence log will consist of either OIG Form III-234/2 (Investigations Division Evidence Log) pages placed in a binder or an electronic logging system. The log must be kept in the designated evidence facility. An example of an evidence log page is at Appendix B.
- Only the primary and alternate evidence custodians may make log entries. Agents wanting to place items into evidence will complete the appropriate blocks of the ECD and hand deliver the evidence to the evidence custodian (agents in domicile offices will mail their evidence to the evidence custodian in the field office). The evidence custodian will assign a log number for the item of evidence and sign the "Received by" block in the chain of custody section prior to securing the evidence.
- D. Evidence Bags. When appropriate, evidence will be placed into a plastic or paper bag and the bag sealed. An adhesive evidence seal will be placed across the opening of the bag, and an adhesive evidence label will be placed on the center portion of the bag. Examples of an evidence seal and evidence label are at Appendix C.

234.9 Evidence Storage and Inventory Procedures.

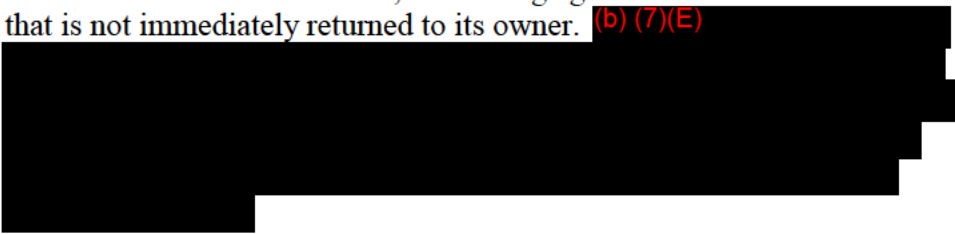
- A. Storage Procedures. The primary evidence custodian will ensure that all evidence stored in the office evidence facility is properly identified, logged, and organized to ensure prompt retrievability. Evidence packaging material may be stored in the evidence facility and made available to agents as needed. Care should be taken to protect evidence from insect or rodent damage, humidity, and other potentially destructive elements.
- B. Special Storage Problems. Some evidence may present storage problems due to its sensitive nature, size, or value. Nevertheless, only the primary and alternate evidence custodians will have unescorted access to any facility or safe used to secure such evidence.
- (1) Grand jury material submitted as evidence either must be sealed in an opaque envelope or box with the outside of the container clearly marked "grand jury material" or must have the evidence custodian(s) added to the grand jury access list by the case agent. The grand jury material must then be stored separately from other evidence. See also the Inspector General Manual, Volume III, Chapter 231 (III-231).

(2) (b) (7)(E)

(b) (7)(E)



- C. Evidence Inventories. The primary and alternate evidence custodians must conduct an inventory annually and whenever either evidence custodian is replaced. Both the new and former evidence custodian must sign the chain of custody section of all ECDs on which the outgoing evidence custodian signed as the last receiver.
- (1) Both evidence custodians should be present during the inventory. The individuals conducting the inventory will compare log entries with items on hand to ensure that all items are accounted for and logged in and that all log and ECD entries are accurate and complete. The results shall be recorded on a separate page in the evidence log. A copy of the inventory shall be forwarded to the SAC of the affected field office.
 - (2) Additionally, inventories are an opportunity to inspect the physical security of evidence facilities and containers and to view evidence for any environmental or other damage.
 - (3) INV Headquarters staff will periodically visit field offices to conduct office reviews, including inspecting evidence inventory records and evidence facility procedures as part of the review. Also, on occasion, personnel from another OIG may visit a DOJ OIG field office as part of a “peer review” and may also request to review office evidence procedures. These personnel may inspect the evidence log and physically confirm the evidence stored but must be escorted while inside the evidence facility.
- 234.10 Special Considerations Regarding Genuine Currency. In addition to the general evidence handling policy and procedures outlined above, the following policy and procedures apply to genuine currency.

- A. Seizing and Counting Genuine Currency. During an investigation, genuine currency may be seized or otherwise come into the custody of an agent as evidence of a crime or for simple safeguarding of property.
- (1) In all cases, when agents take custody of genuine currency, both the seizing agent and a witness to the seizure will separately count the money at the scene when practical. The seizing agent will specify (on the return of the search warrant) the amount of money that was seized. If the money was obtained without search warrant, the seizing agent will complete OIG Form III-233/2 (Receipt for Cash and Other Items) and annotate the amount of money that was seized. The counted money will then be inventoried on an ECD prior to being placed into evidence. If the number of notes is extensive, prepare an MOI listing all serial numbers by denomination or use "continuation" ECDs. Both persons counting the money must sign the ECD, one as the "Seizing Special Agent" and the other as the "Witness," to certify the separate counting of the money.
 - (2) Within 24 hours of the seizure, the seizing agent shall surrender all currency that is not immediately returned to its owner. (b) (7)(E)

 - (3) The case agent will also promptly notify the office SAC and assigned prosecutor of any genuine currency taken into custody by the OIG during an investigation. A memorandum to the case file will certify this notification.
- B. Joint Investigation Seizures. When another agency takes possession of genuine currency during a joint investigation, no OIG inventory is required. However, if an OIG agent was involved in the seizure of the money, the circumstances of the agent's involvement and the disposition of the money will be fully documented in an MOI to the relating case file.
- C. Defendants in Possession of Genuine Currency. In most cases, genuine currency found in the possession of an arrested person need not be retained as evidence. The presence of money on a prisoner's person can readily be proven by agent witness accounts without the need of the actual currency. However, if money is taken from an arrested person, even if only to verify the amount, the prisoner and another witness must be present during the counting. When the currency is not retained as evidence, control of the money should be transferred back to the defendant or delivered to the place of the defendant's incarceration. In either case, a receipt will be obtained for inclusion in the case file. OIG Form III 233/2 will be used for this purpose.

For those occasions when genuine currency must be taken from a defendant for safekeeping or as evidence of a crime, the money will be counted, inventoried, packaged, and surrendered to the evidence custodian as described above.

D. Seizures of Large or Unusual Amounts of Cash. (b) (7)(E)

[REDACTED]

(1) Even if large amounts of money are not subject to seizure by the OIG as evidence or for safekeeping, large amounts of cash encountered by agents may be subject to a “jeopardy assessment” by the Internal Revenue Service (IRS). The IRS is the only entity empowered by law to seize money based upon a jeopardy assessment. Generally, the IRS will authorize the seizure of large amounts of cash where there is probable cause to believe the money was obtained in a manner that evaded the payment of federal income (or other federal) taxes.

(2) (b) (7)(E)

[REDACTED]

(3) (b) (7)(E)

[REDACTED]

E. Forfeiture of Money to Cover Fines or Victim Compensation. The OIG does not have statutory authority for the forfeiture of seized money. However, if the money is not subject to seizure as evidence, consideration may be given to using other legitimate asset forfeiture statutes, such as those dealing with controlled substances or tax violations, after consultation with the agency authorized to enforce those statutes.

Once the OIG seizes genuine currency, the prosecutor assigned to the case must be made aware that the money is in evidence. The prosecutor should then advise the judge handling the case at sentencing that seized currency is available to satisfy any fine or victim compensation ordered by the court. It is essential that the prosecutor resolves the disposition of seized currency with the judge through judicial process at sentencing, as the government may not obtain forfeiture at a later date under any OIG authority.

- F. Storage of Genuine Currency Pending Final Disposition. (b) (7)(E)

[REDACTED]

234.11 Evidence Shipment Procedures.

- A. Packaging. Do not identify items as evidence on the outside packaging or labels. Double wrap evidence and mark with the caption "To Be Opened by Evidence Custodian Only" on the inner wrapping or label.
- B. Shipment Between DOJ OIG Offices. All evidence should be sent to the appropriate primary evidence custodian. Telephone the evidence custodian to alert him or her that evidence has been shipped.
- (1) Evidence will be sent via registered U.S. mail, Federal Express, or similar traceable means. The evidence custodian will record the registration or tracking number in the evidence log. Ask the local post office for assistance with questions regarding the mailing of specific items (for example, guns or ammunition).
 - (2) The receiving evidence custodian shall promptly telephone the sending evidence custodian to notify him or her that the package has been received.
- C. Shipment to Laboratories. When forwarding evidence to another law enforcement agency or approved forensic laboratory for examination, packages shall be sent from one official address to another, following the addressing and shipping instructions provided by the laboratory. All evidence will be shipped to forensic labs or other law enforcement agencies via USPS registered mail or like traceable means.

234.12 Evidence Disposition. Generally, evidence may not be returned, destroyed, or otherwise disposed of without approval by a designated Assistant United States Attorney (AUSA) or court official. Recognizing that not all OIG investigative matters result in actions involving federal prosecutors, evidence disposition may be based on instructions from state prosecutors in appropriate cases. In cases where criminal prosecution is declined or the matter is pursued purely in an administrative forum, appropriate disposition of evidence may be authorized in writing by the field office SAC in accordance with the following guidelines. Upon receiving disposition instructions, the evidence custodian will release the evidence to be disposed of to the case agent. The case agent will ensure the prompt and proper disposal of the evidence.

- A. Release of Evidence for Trial. The case agent is responsible for signing out evidence for trial. The ECD will remain affixed to the item of evidence. The case agent should advise the receiving trial counsel or authorized officer to maintain security over the evidence and preserve the chain of custody by completing appropriate entries on the ECD.

- B. Return of Evidence to Owner. The case agent is responsible for returning evidence directly to the rightful owner or lawful custodian. The return of evidence will be documented via the “Chain of Custody” portion of the ECD, and an EDD will be completed.
- (1) Personal return of evidence is preferred. Upon return of the evidence, the agent will obtain the signature of the owner or owner’s representative on an EDD.
 - (2) Where personal return is not practicable, items may be returned via registered U.S. mail, Federal Express, or similar means. The case agent will package the item(s) for mailing and mail the package, record the registered mail information on the ECD, and then file the ECD and the registered mail or Federal Express receipt in the case file. Upon receiving the delivery confirmation receipt, the case agent will also file it in the case folder.
- C. Final Disposition Guidelines. The evidence custodian must clearly document the final disposition on the ECD and in the evidence log. The case agent will file the closed-out ECD along with the EDD within the investigative case folder.

Final disposition of evidence will be in accordance with the following guidelines:

- (1) All private property will be returned to the owner (after AUSA approval) unless:
 - a. the property is contraband or its possession is prohibited by law or regulation;
 - b. the owner is unknown, in which case the item will be declared lost, abandoned, or unclaimed and disposed of accordingly. The field office SAC will decide on the final disposition in consultation with the AUSA, where appropriate, or the SAC, Investigative Support Branch, INV Headquarters; or
 - c. the owner's desire that the property not be returned has been documented. The field office SAC will decide on the final disposition in consultation with the AUSA where appropriate.
- (2) All government property will be returned to the appropriate property custodian.
- (3) Upon release from evidence, all illegal drugs will be destroyed, and their destruction must be witnessed and documented by MOI and EDD. The MOI must include the case number; ECD number; and when, where, and how the drugs were destroyed and who witnessed the destruction. At least two agents will witness the destruction of drug evidence.

- (4) Disposal of genuine currency or negotiable instruments seized as evidence requires special handling. Currency is disposed of through court order, return to owner, or abandonment procedures.
 - a. Court Order. For cases resulting in federal criminal or civil court action, before sentencing or final civil disposition, the case agent should ensure that the handling AUSA prepares a motion requesting that the judge order the appropriate disposal of currency or negotiable instruments. At the time of sentencing, the judge may order that the seized money be used to satisfy a fine, pay restitution, or become the property of the U.S. Government. The court order should also direct to whom the money must be delivered. The OIG may convert seized cash to a cashier's check or money order to fulfill the court order.
 - b. Return to Owner. In cases where there is no conviction, prosecution, or IRS seizure, the currency should be returned to the rightful owner in accordance with the procedures outlined in paragraph B above.
 - c. Abandonment. In cases where the rightful owner is unknown and genuine currency is unclaimed by any party or is abandoned, the case agent should contact the SAC, Investigative Support Branch, INV Headquarters. The SAC, Investigative Support Branch, will coordinate with the Office of General Counsel and the Management and Planning Division to arrange for transfer of the money to the U.S. Treasury. Some seized bribe money may fall into this category. The specific procedures for transmitting bribe money or other seized genuine currency to the U.S. Treasury are more fully addressed in paragraphs E and F below.
- (5) When counterfeit U.S. currency or counterfeiting equipment is released from evidence, contact the local office of the U.S. Secret Service for disposition guidance.
- (6) Upon release from evidence, legally obtained weapons shall be returned to their rightful owner. Other weapons shall be appropriately destroyed, made inoperable, or disposed of in accordance with federal property guidelines.
- (7) Only nonconsensual original audio- and videotapes produced through electronic surveillance will be retained if either: actually introduced in court; requested by the defense but not provided; or suppressed by a judge or magistrate. Although consensual recordings may be destroyed after the appeals process has run, nonconsensual recordings (wiretaps) must be maintained for a minimum statutory period of 10 years. Evidence custodians are cautioned to dispose of recorded audio- or videorecordings only after coordinating with the AUSA who handled the case and receiving written

direction. In addition, it is recommended, where practicable, that a certified transcript of the tape or pertinent portions thereof be maintained in the case file.

- (8) When photographs or fingerprint lifts are released from evidence, they will normally be destroyed with the concurrence of the handling AUSA (if applicable) or stored in the case file. The evidence custodian will document the disposition on the ECD and EDD and in the evidence log. The case agent will place the ECD(s) in the case file.
- (9) When final disposition of evidence consists of release to another agency for its investigative or prosecutorial action, the following steps will be taken:
 - a. Obtain approval from the assigned AUSA (when applicable) and the field office SAC for the transfer.
 - b. Complete the ECD and evidence log reflecting the transfer from the OIG to the receiving agency as the final disposition. Ensure that the receiving agency signs for the evidence on an EDD.
 - c. Place the ECD and EDD in the case file.
 - d. Release the evidence to the receiving agency.
- (10) The final disposition of all property seized as evidence (including genuine currency) must be explained in detail in an MOI. Along with the ECD and EDD, this MOI will be attached as an exhibit to the final Report of Investigation for the associated case.

D. Disposition of Bribe Monies and Other Genuine Currency. Cash seized by OIG agents during bribery or other investigations will be disposed of as follows:

- (1) In cases where the subjects have been convicted of bribery and where the seized funds are known to be bribe monies, the U.S. Attorney's Office should file pleadings pursuant to 18 U.S.C. § 3666. When this process is successful, the money will remain in the court registry for 5 years before being transferred to the U.S. Treasury. The case agent must attempt to ensure that the AUSA files the required pleadings in a timely manner, as this is the simplest way for the OIG to dispose of seized bribe money.
- (2) Seized bribe monies may be deposited directly to the U.S. Treasury, via INV Headquarters, in the following situations:
 - a. Where substantial evidence exists that a bribe was paid to a government official but the subject becomes a fugitive and the likelihood or timing of prosecution is now questionable;

Where the subjects of an investigation are fugitives and the case meets the OIG criteria for closure and it is unknown if a trial will ever take place, procedures must ensure that if the matter is ever brought to trial, the bribe monies will be available as evidence. This can be accomplished by photographing the original seized cash before converting the money to a cashier's check for deposit with the U.S. Treasury. The check should also be photographed and the check number noted. The photographs should then be filed with the detailed inventory of the money in the relating case folder. Records must be maintained regarding the amount of seized bribe monies associated with a particular case. If individuals file a claim or seek the return of the money, this process will allow identification of the appropriate funds in order to respond to the claim. (See paragraphs E and F below for the specific procedures for transferring funds to the U.S. Treasury.)

- b. Where the subject has been successfully prosecuted or has submitted a guilty plea yet there is no specific resolution of the bribe monies paid to a government official and the prosecuting attorney has declined to address the disposition of monies with the court.

- E. Procedures for Requesting Approval for Direct Deposit to the U.S. Treasury. Requests must be made by memorandum from the field office SAC to the SAC, Investigative Support Branch, INV Headquarters, who will consult with the Management and Planning Division and the Office of General Counsel. The memorandum will include the following information: the case numbers and dates closed; the amount of bribe monies seized in each case (list each seizure individually with the date seized); the status of the major defendants in the case, including the status of defendants from whom funds were seized; and the reason the office has been unable to otherwise lawfully dispose of the funds. See Appendix D for a sample request memorandum. If approved, INV Headquarters will notify the field office SAC via memorandum.
- F. Procedures for Transmitting Bribe Monies or Other Genuine Currency. When the field office receives written approval from headquarters to deposit seized bribe monies with the U.S. Treasury, (b) (7)(E) Two agents must then immediately take the funds to a financial institution and obtain a cashier's check. If more than one seizure is involved, all the seized money should be combined together into one cashier's check issued payable to the U.S. Treasury. However, a separate check must be obtained for funds involved in a fugitive case as described in paragraph D(2)a above. When converting seized genuine currency to a cashier's check, the agent should identify himself or herself as a law enforcement officer and provide DOJ's Employer Identification Number 53-0205705 for inclusion in any currency transaction report the bank might be required to file.

- (1) The check will be sent via Federal Express or other like traceable means to:

U.S. Department of Justice
Office of the Inspector General, Investigations Division
ATTN: _____(name), SAC/Investigative Support Branch
1425 New York Avenue, NW, Suite 7100
Washington, DC 20005
Tel. (202) 616-4760

- (2) The cashier's check must be accompanied by a cover memorandum from the field office SAC and a completed OIG Form III-234/3 (Transmittal of Bribe Monies) (Appendix E). The cover memorandum from the SAC will reference the memorandum from INV Headquarters granting approval to transmit the funds; state that these monies were unlawfully paid as a bribe to a government official; and provide the case number, date, and status of judicial action (for example, prosecution declined, fugitive, conviction, guilty plea).
- (3) The OIG Form III-234/3 will serve as the inventory tracking record for the monies contained in the check, as it captures the OIG case number, the name(s) of the individuals who paid the bribes or from whom the monies were seized (if known), and the amount of money specific to each transaction. Upon receipt of the cover memorandum, cashier's check, and transmittal form, the OIG financial manager will certify receipt of the funds, assign a control number to the transaction, and return a signed copy of the transmittal form to the SAC for field office records.

- G. Prolonged Evidence Retention. Occasionally, the U.S. Attorney's Office may request evidence be held pending judicial review or appeal. In such instances, maintain custody of the evidence until written release authorization from the assigned AUSA is obtained. Record the reason for continuing custody, along with the name and telephone number of the requester, in the evidence log.

234.13 Special Evidentiary Considerations Regarding Investigations of Sexual Abuse in Confinement Settings.

- A. Initial Preservation of Evidence. If an assault occurred very recently and if the potential exists for the recovery of forensic evidence, the investigating agent will contact the institution and ensure that the crime scene is preserved and protected until appropriate steps can be taken to collect any evidence. (See also Appendix F for definitions of sexual abuse and harassment terms in the Prison Rape Elimination Act.)

B. Medical Examinations.

(1)

(b) (7)(E)

A large black rectangular redaction box covers the majority of the text for item (1). The text "(b) (7)(E)" is visible in red at the top left corner of the redacted area.

(2)

(b) (7)(E)

A large black rectangular redaction box covers the majority of the text for item (2). The text "(b) (7)(E)" is visible in red at the top left corner of the redacted area.

- (3) Medical forensic examinations of the victim (and the subject, with a warrant or consent) will be conducted in accordance with the standards set forth in A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/Adolescents, DOJ Office of Violence Against Women, second edition, April 2013, <https://www.ncjrs.gov/pdffiles1/ovw/241903.pdf>.

C. Conducting Forensic Crime Scene Investigation Involving Biological Evidence.

(b) (7)(E)

A large black rectangular redaction box covers the entire text for section C. The text "(b) (7)(E)" is visible in red at the top left corner of the redacted area.

(b) (7)(E)



D. Handling Biological Evidence.

(b) (7)(E)



E. Detecting and Testing Forensic Evidence.

- (1) Laboratory testing of forensic and biological evidence can be conducted by any accredited forensic laboratory, such as those run by the FBI, ATF, and most state law enforcement agencies.

- (2) (b) (7)(E) [REDACTED]
- (3) (b) (7)(E) [REDACTED]
- (4) There are several tests for the presence of semen and sperm, such as:
- a. P30 test — P30 is a protein specific to semen. Testing for P30 does not require the presence of sperm, so the test works even if the offender had a vasectomy.
 - b. Acid phosphatase (AP) — this is a presumptive test. There is generally a large amount of the enzyme AP in human sperm.
 - c. Microscopic identification of sperm cells — this is a visual test.
- (5) DNA testing will confirm the ownership of cells collected, but it does not discriminate concerning the type of cell tested. Therefore, a P30 test may be required to determine the presence of semen, along with a DNA test to determine the ownership of the sample. A buccal swab or similar DNA retrieval method will be needed for comparison unless the subject's DNA is already on file with the National DNA Database because of an arrest or other collection circumstance.

APPENDIX A

Evidence Custody Document
(OIG Form III-234/1)

Evidence Disposition Document
(OIG Form III-234/4)

EVIDENCE CUSTODY

OFFICE	CASE #	LOG #	DATE AND TIME OF SEIZURE	
PROPERTY SEIZED FROM		LOCATION OF SEIZURE		
ITEM	DESCRIPTION OF THE PROPERTY SEIZED			
NAME AND SIGNATURE OF WITNESS		NAME AND SIGNATURE OF SEIZING SPECIAL AGENT		
CHAIN OF CUSTODY				
ITEM	DATE/TIME	RELEASED BY <i>(Name and Signature)</i>	RECEIVED BY <i>(Name and Signature)</i>	PURPOSE

EVIDENCE DISPOSITION DOCUMENT

NAME OF AUTHORIZING OFFICIAL	TITLE AND TELEPHONE NUMBER	DATE	CASE NUMBER
DISPOSITION ORDERED <i>(check one)</i>	DESCRIPTION OF ITEM		
<input type="checkbox"/> RETURN <input type="checkbox"/> DESTROY <input type="checkbox"/> OTHER <i>(specify)</i>			
EVIDENCE RETURNED/OTHER ACTION			
NAME AND SIGNATURE OF SPECIAL AGENT RELEASING THE EVIDENCE			
NAME OF PERSON RECEIVING EVIDENCE	DATE AND SIGNATURE OF RECIPIENT		
ADDRESS	TELEPHONE NUMBER		
EVIDENCE DESTROYED			
METHOD USED			DATE
NAME AND SIGNATURE OF PERSON WHO DESTROYED THE EVIDENCE			DATE
NAME AND SIGNATURE OF WITNESS			DATE

Investigations Division Evidence Log

(OIG Form III-234/2)

APPENDIX C

Evidence Bag Seal and Label

(b) (7)(E)



Sample Memorandum Request to Dispose of Seized Funds

May 10, 2004

MEMORANDUM FOR Willie Haynes
Special Agent in Charge
Investigative Support Branch
Investigations Division Headquarters

THROUGH: Ralph F. Paige, Special Agent in Charge
New York Field Office

FROM: (b) (6), (b) (7)(C), Special Agent
New York Field Office

SUBJECT: Request to Dispose of Seized Funds

The New York Field Office is requesting assistance from the Special Agent in Charge, Investigative Support Branch, Investigations Division Headquarters, to dispose of funds in accordance with Inspector General Manual Chapter III-234 (Subsections 234.12D, "Disposition of Bribe Monies and Other Genuine Currency," and 234.12E, "Procedures for Requesting Approval for Direct Deposit to the U.S. Treasury").

It is necessary to deposit the funds with the U.S. Treasury because the subject government official receiving a bribe has been successfully prosecuted. However, there is no specific resolution of the bribe monies received and subsequently seized, and the prosecuting attorney has declined to address the disposition of the monies with the court.

<u>Amount of Funds</u>	<u>Date Seized</u>	<u>Defendant</u>
\$100	July 14, 2002	John Doe
\$70	July 15, 2002	John Doe
\$7,174	July 18, 2002	Robert Smith

Total: \$7,344

<u>OIG Case Number</u>	<u>Date Closed</u>
(b) (6), (b) (7)(C)	November 7, 2002

Case Status:

This investigation was based on allegations that Immigration Clerks Jane Doe, Joe Brown, and John Doe, assigned to the ICE New York District Office, conspired with Robert Smith, a foreign national, and others to provide genuine ICE documents to individuals not entitled to them.

Both Doe and Smith admitted that the monies seized were bribe payments. Doe, Brown, Smith, and Doe II subsequently pleaded guilty in United States District Court, Southern District of New York, and were sentenced by a U.S. district court judge. However, the United States Attorney's Office did not address disposition of the seized bribe monies with the court.

The New York Field Office will await approval from headquarters before transmittal of the bribe monies to the OIG Financial Manager for transfer to the U.S. Treasury. If you need further information or have any questions, please contact Special Agent (b) (6), (b) (7)(C) at (718) 553-7520.

Transmittal of Bribe Monies
(OIG Form III-234/3)

Transmittal of Bribe Monies — Continuation
(OIG Form III-234/3A)

I. FUNDS INFORMATION

OIG Control No. _____
(Assigned by M&P Budget and Planning)

Cashier's Check No. or Money Order No. _____ Amount \$ _____

Case No.	Subject	Amount \$
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Subtotal, this page... \$ _____

Subtotal, additional sheets (attached)... \$ _____

TOTAL (must equal total of check/money order)... \$ _____

List all cases and subjects separately. Use OIG Form III-234/3A — Continuation if necessary

II. REMITTER INFORMATION

Agent: _____ Signature: _____ Office: _____

III. REMARKS (Attach check or money order payable to "U.S. Treasury" here)

IV. CERTIFICATION

I certify that I received \$ _____ (write out _____).

(Financial Manager or Designee)

(Signature)

(Date)

APPENDIX F

Definitions of Terms in the Prison Rape Elimination Act

DEFINITIONS OF TERMS IN THE PRISON RAPE ELIMINATION ACT

The definition of *sexual abuse of an inmate, detainee, or resident by a staff member, contractor, or volunteer* includes any of the following acts, with or without consent of the inmate, detainee, or resident:

- (1) contact between the penis and the vulva or the penis and the anus, including penetration, however slight;
- (2) contact between the mouth and the penis, vulva, or anus;
- (3) contact between the mouth and any body part where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (4) penetration of the anal or genital opening, however slight, by a hand, finger, object, or other instrument, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (5) any other intentional contact, either directly or through the clothing, of or with the genitalia, anus, groin, breast, inner thigh, or the buttocks, that is unrelated to official duties or where the staff member, contractor, or volunteer has the intent to abuse, arouse, or gratify sexual desire;
- (6) any attempt, threat, or request by a staff member, contractor, or volunteer to engage in the activities described in paragraphs (1)-(5);
- (7) any display by a staff member, contractor, or volunteer of his or her uncovered genitalia, buttocks, or breast in the presence of an inmate, detainee, or resident, and
- (8) voyeurism by a staff member, contractor, or volunteer.

Voyeurism by a staff member, contractor, or volunteer means an invasion of privacy of an inmate, detainee, or resident by staff for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring an inmate to expose his or her buttocks, genitals, or breasts; or taking images of all or part of an inmate's naked body or of an inmate performing bodily functions.

Sexual harassment in a confinement setting includes:

- (1) repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
- (2) repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures.

INSPECTOR GENERAL MANUAL
Volume III, Chapter 234
Evidence
Revisions

This chapter was previously revised on April 23, 2007, and originally issued on January 25, 1995. This chapter was rewritten to reflect updates and changes in policies, laws, and guidelines.

This chapter revision includes an inserted revised policy, approved by the Inspector General or his Designee, issued July 9, 2014:

This policy addition is in conformance with the Prison Rape Elimination Act (PREA), Public Law 108-79, which was passed unanimously by Congress in 2003, and AG Order No. RIN 1105-AB34, as codified in the Code of Federal Regulations (C.F.R.), Title 28, Part 115, on May 16, 2012. (See also www.ojp.usdoj.gov/programs/pdfs/prea_final_rule.pdf.)

234.13: Adds guidance concerning processing and investigation of allegations of sexual abuse in confinement settings (Policy Memorandum FY 14-POL-03).

Appendix F: Adds Definitions of Terms in the Prison Rape Elimination Act (Policy Memorandum FY 14-POL-03).

Changes, additions, and deletions in guidance issued July 1, 2009, appear in the following sections.

234.8B(1) and (2): Updating labels of ECD blocks.

234.9B(1): Adds policy on separate storage of grand jury material.

234.10A(1): Adds clarification on signing the ECD.

234.10D: Adds clarification regarding transporting currency.

234.12B: Adds EDD completion guidance regarding returning evidence.

234.12C(1)b: Adds the Investigative Support Branch as a disposition consultant.

234.12C(3), (8), and (9)c: Adds EDD guidance.

Appendix A: Adds “Name and Signature” guidance to OIG Form III-234/1.
Adds an item description column to the Disposition Ordered row in OIG Form III-234/4.

Appendix D: Changes the appendix title

300.1 Policy. This chapter establishes administrative policies and procedures to facilitate the orderly operation of the Investigations Division (INV), Office of the Inspector General (OIG).

300.2 References.

- A. The Inspector General Act of 1978, as amended;
- B. 41 C.F.R. § 202-9.103, which directs each agency to provide policy and procedural guidance through an established directives program; and

300.3 Scope. The provisions of this chapter apply to all employees in the OIG INV.

300.4 Definitions.

A. Serious Incident. A serious incidents is defined as follows:

- (1) an on-duty or work-related incident involving serious bodily injury requiring medical attention or involving a death;
- (2) an incident involving the use of a firearm: shooting incidents accidental discharge, and loss or theft of a firearm (further described in Inspector General Manual (IGM) Volume III, Chapter 201, Firearms and Defensive Tactics);
- (3) an on-duty or work-related incident involving significant property damage;
- (4) an accident or incident of a government-owned or leased vehicle or a vehicle rented for government use that involve death, serious bodily injury, or substantial property damage;
- (5) an arrest or instance in which the employee has been taken into custody, held for investigation, or detained for questioning, regardless of whether the employee was in a duty or non-duty status at the time of the occurrence; or
- (6) an unusual or non-routine incident that may result in the immediate attention of the media.

B. Traumatic Incident. An incident that causes stress sufficient to overwhelm the coping skills of an individual or group. The event can have the potential to interfere with the ability to function either at the scene of the incident or thereafter.

C. Post-Traumatic Stress Disorder. An anxiety disorder that can result from exposure to short-term severe stress or from the long-term buildup of repetitive and prolonged milder stress.

- D. Agent-Involved Shooting Incident. A shooting incident that occurs in the line-of-duty that causes death or serious bodily injury to any person.

300.5 Responsibilities in the Event of a Serious Incident.

Following the initial notification of a serious incident, applicable sections of the IGM will be controlling as they apply to further notifications, reports, and other procedures. For example, an employee involved in a shooting will follow the protocols set forth in IGM Volume III, Chapter 201, Firearms and Defensive Tactics; an employee detained for questioning in a criminal matter will follow the protocols set forth in IGM Volume I, Chapter 030, Standards of Conduct.

The timely notification of a serious incident to INV Headquarters allows for immediate actions to be taken, for example, referring the employee to the Employee Assistance Program and convening a shooting review team.

- A. Notification by Employee. An employee is required to notify their Assistant Special Agent in Charge or first-line supervisor as soon as possible following a serious incident. Serious incidents, such as those involving a shooting, may require further actions, as provided for in § 300.6.
- B. Field Supervisor. If an on-duty agent is involved in a serious or traumatic incident, including those involving bodily injury or death, an OIG supervisor should be dispatched to the scene or the location to which an involved agent has been taken. The supervisor should notify the Assistant Inspector General for INV and implement the traumatic incident procedures in a timely manner.

The OIG supervisor will ensure traumatic incident response treatment is offered to agents or involved OIG persons experiencing traumatic incident stress or post-traumatic stress disorder by notifying the Justice Management Division for assistance of the Employee Assistance Program.

- C. INV Headquarters. Upon learning of a serious or traumatic incident, the Assistant Inspector General for INV will notify the Inspector General of all available facts. Subsequent INV Headquarters responses should include, as appropriate, the following:
- (1) informing the Office of General Counsel and the Management and Planning Division (M&P) of the incident.
 - (2) sending an INV Headquarters manager to the incident site.
 - (3) ensuring that the affected field office has sufficient managerial and administrative support.

- (4) notifying INV employees of the incident.
- (5) contacting Justice Management Division to arrange for Employee Assistance Program support. Peer support teams, coordinated through the Employee Assistance Program, may be composed of individuals from the Federal Bureau of Investigation, Drug Enforcement Administration, or other components.
- (6) coordinating any media responses with the Senior Counsel to the Inspector General or the designee if the incident involves a shooting incident.

300.6 Procedures.

A. Shooting Incident Procedures.

Shooting incident procedures should be followed in conjunction with those delineated in IGM III, Chapter 201. Field Supervisor Initial Responsibilities:

An OIG supervisor will be dispatched to the scene of an agent-involved shooting or the location to which an involved agent has been taken. The OIG supervisor will assume primary responsibility for caring for involved personnel and will provide supportive face-to-face communication, helping to alleviate fear regarding the agency's reaction to the incident. The supervisor does not have to comment on the incident but will show general care and be supportive of the agent. The supervisor should take the following actions:

- (1) Notify the Assistant Inspector General for INV.
- (2) Adapt actions in accordance with the state or local authority's handling of the shooting investigation and need for medical treatment.
- (3) Arrange for the involved agent to leave the area as soon as possible but in cooperation with the authorities investigating the shooting.
- (4) Move the involved agent to a quiet, non-public area away from the immediate scene of the incident if the involved agent is required to remain on the scene but has no immediate duties to fulfill. A counselor or other supportive person should remain with the involved agent but should not discuss details of the incident with the involved agent.
- (5) Supervisors should keep the following guidance in mind when meeting with the involved agent.
 - a. The agent should not be provided caffeine or other stimulants or depressants unless administered by medical personnel.

- b. The supervisor should ask minimal preliminary questions about the incident but should not press for details. The supervisor should also advise the agent that a more detailed debriefing will be conducted at a later time. Before undergoing a detailed interview, the agent should have some recovery time in a secure setting.
 - c. The supervisor should encourage the involved agent to notify their family about the incident as soon as possible.
 - d. The supervisor should inform the agent that a shooting incident review will be conducted, as stated in IGM Volume III Chapter 201.17.
 - e. The agent should be informed that they can seek legal counsel.
 - f. The agent should be informed that they should not discuss the incident with anyone during the pendency of the preliminary investigation other than a personal or agency attorney, association representative, or agency investigator until the conclusion of the preliminary investigation.
- (6) Determine, with the agreement of the law enforcement agency that has jurisdiction to investigate the shooting incident, whether the circumstances require that the agent's duty weapon be taken for laboratory analysis. The SAC, Investigative Support Branch, INV Headquarters should be consulted before any OIG weapons are transferred to state or local authorities as evidence or for ballistics tests. If a duty weapon is taken, the supervisor will:
- a. Take custody of the weapon in a discrete manner.
 - b. Advise the agent that the weapon will be either returned at a later time or replaced. (Another weapon will be issued immediately unless there is cause not to issue one.)
 - c. Treat the weapon and spent cartridges as evidence and maintain them at the field office if the cognizant law enforcement agency does not request the weapon and spent cartridges. The weapon will be held until it is needed for laboratory analysis or until criminal, civil, and administrative actions are completed.
- (7) Ensure that initial contact with the family of an agent who has been killed or injured is in-person and by an appropriate OIG representative. Considering all the circumstances, one or more of the following representatives should be considered for making the initial contact: the agent's Special Agent in Charge, or Assistant Special Agent in Charge, or an OIG agent known to the family, if it is determined desirable for the agent known to the family to be involved in making the initial contact. The notifying agent or manager will

personally notify the family and arrange for the family to be transported to the hospital or other suitable location. Field office personnel should also be notified of the agent's condition so they can respond to inquiries from family members who call the field office. It is of the highest priority that the family notification be made as soon as practicable, and that every effort be made to ensure that the agent's family learns of the incident first and directly from the OIG, not from a public source. The supervisor may request assistance from the Employee Assistance Program in notifying the family.

- (8) Interact with the agent and all involved personnel in a manner that acknowledges the stress caused by the incident.
- (9) Make a referral to the presiding U.S. Attorney's Office if there is a possible violation of 18 U.S.C. § 111 (assaulting, resisting, or impeding certain officers or employees) or § 1114 (protection of officers and employees of the United States).

B. After-Incident Procedures.

- (1) Pending an INV evaluation, involved personnel may be relieved of active investigative duties but remain available for administrative duties. Alternatively, involved employees may be placed on administrative leave for a period of time to allow them time to process the emotional impact of the event. M&P will provide specific advice concerning administrative leave appropriate for the situation.
- (2) Any agent involved in a shooting is required to participate in a traumatic incident stress debriefing conducted by a knowledgeable mental health professional. The debriefing should take place as soon after the shooting as practical, generally within 24- to 72-hours. Fitness for duty and any need for follow-up sessions will be determined by the mental health professional.
- (3) A supervisor should brief the relevant Special Agent in Charge affected field office regarding the incident to prevent office discussion from occurring. The Assistant Inspector General for INV (or another individual specifically designated) will release a brief account of the incident by e-mail to all offices.
- (4) Administrative or other investigations related to the incident will be completed as expeditiously as possible and in coordination with INV Headquarters. The involved agent will be advised of the outcome of all investigations.
- (5) All OIG personnel involved in a shooting incident should be informed that they should not discuss the incident with others during the pendency of the

investigation of the incident, other than a personal or agency attorney, association representative, or agency investigator.

- (6) The OIG Senior Counsel or designee will address inquiries from the news media and release a statement, if appropriate, pertaining to the incident. The best interests of the agent will be considered prior to making any news media releases. If a field supervisor is authorized to make a statement to the news media, they should not vary from the approved statement provided by the OIG.

C. Injured Agent Procedures. If an agent is seriously injured on duty and expected to remain hospitalized, the field supervisor should:

- (1) Assign a senior agent to the hospital. The agent will act as a liaison to coordinate the following:
 - a. security and privacy of the injured agent,
 - b. inquiries from OIG and other law enforcement officers,
 - c. news media inquiries,
 - d. visiting hours with office personnel.
- (2) Ensure additional items of evidence are properly secured by the hospital. When in doubt, treat items as evidence.
- (3) Keep OIG management and office personnel apprised of the condition of the agent.
- (4) Assist the agent in coordinating with M&P to obtain various employee benefits. A M&P benefits specialist will provide assistance and guidance in this area.

D. Management Follow-Up. Post-Traumatic Stress Disorder may not be evident immediately, or the agent may attempt to hide a problem.

- (1) Each supervisor is responsible for monitoring the behavior of office personnel for symptoms of Post-Traumatic Stress Disorder. The following are some symptoms that supervisors should be aware of and recognize:
 - a. *Re-experiencing the trauma*: flashbacks, nightmares, intrusive memories, and exaggerated emotional and physical reactions to triggers that remind the person of the trauma.

- b. *Emotional numbing*: feeling detached, lack of emotions (especially positive ones), and loss of interest in activities.
 - c. *Avoidance*: avoiding activities, people, or places that remind the person of the trauma.
 - d. *Increased arousal*: difficulty sleeping and concentrating, irritability, hyper-vigilance (being on guard), and exaggerated startle response.
- (2) A supervisor may require an agent to seek assistance or counseling from a mental health professional. This action may be taken upon a reasonable belief that stress may be disrupting the agent's job performance or ability to carry a firearm.

001.1 Policy. This chapter describes the mission and responsibilities of Evaluation and Inspections Division (E&I) of the Department of Justice (Department) Office of the Inspector General (OIG).

The Assistant Inspector General (AIG) for E&I and E&I's management staff will clearly communicate the mission and responsibilities to employees, the Department, the Executive Branch, and Congress.

All evaluations and inspections adhere to internal policy and guidelines issued by the OIG, and generally conform to the standards issued by the Council of Inspectors General on Integrity and Efficiency.

001.2 Reference.

- A. The Inspector General Act, as amended (Public Law 100-504, October 18, 1988);
- B. The Inspector General Reform Act of 2008 (Public Law 110-409, October 14, 2008).

001.3 Scope. Provisions of this chapter apply to E&I.

001.4 Mission Statement. E&I conducts program reviews to assess and improve the implementation and effectiveness of Department programs and operations. In addition to assessing Department programs, E&I conducts reviews requested by the Inspector General, Deputy Inspector General, or senior Department management of issues that need immediate attention.

001.5 Responsibilities. The primary responsibilities of E&I include:

- A. Conducting evaluations and inspections of field and headquarters entities and Department programs and functions to evaluate the effectiveness, efficiency, and economy of Department operations.
- B. Documenting and reporting all evaluation and inspection findings of Department programs and operations with the related recommendations for improvement and required corrective actions.
- C. Maintaining a documented follow-up system on all evaluation and inspection reports of Department programs and operations to ensure the resolution of recommendations and the implementation of required corrective actions.
- D. Working to identify and report on situations and patterns indicating waste or fraud in Department programs and operations.
- E. Maintaining an active interchange with other components of the OIG to enhance coordination and cooperation.

Revisions

This chapter was originally issued on April 5, 1991, and was revised on June 3, 1993, and again on September 12, 2003.

In this version, this chapter was renamed from Mission, Organization, and Functions.

- 003.1 Policy. This redelegation states the authority and responsibilities of the Office of the Inspector General (OIG), Evaluation and Inspections (E&I) Division.
- 003.2 Reference.
- A. Inspector General Act as amended;
 - B. Attorney General Order No. 1341-1989, Delegating Certain Authorities to the Inspector General, Department of Justice (April 14, 1989);
 - C. Inspector General Manual (IGM), Volume I, Chapter 002, Mission, Organization, and Functions; and
 - D. IGM, Volume I, Chapter 003, Delegation of Authorities.
- 003.3 Scope. This chapter applies to the E&I Division.
- 003.4 Procedures. When designated to act on behalf of the Inspector General, the Deputy Assistant Inspector General for E&I (DAIG/E&I) may exercise the administrative and operational authorities described in Volume I, Chapter 002, § 002.8G and in accordance with additional applicable chapters in the Inspector General Manual. Authorities not specifically delegated in this chapter or elsewhere in the IGM are retained by the Inspector General and Assistant Inspector General for E&I (AIG/E&I).
- 003.5 Responsibilities.
- A. Authorities Retained by the E&I Directors. The Directors within the E&I Division are delegated the following responsibilities and functions to:
 - (1) Oversee and conduct evaluations and inspections of Department of Justice (DOJ) programs and operations;
 - (2) Oversee the written product documenting E&I report findings and resolution activities;
 - (3) Work with officials of reviewed entities throughout the review to keep them apprised of the review progress;
 - (4) Oversee the internal control process for E&I;
 - (5) Assist in the development and implementation of program goals, policies, procedures, and performance;

- (6) Approve annual, sick, and other forms of leave permitted by law, with the exception of advanced leave, for all subordinates subject to leave policies and regulations of the OIG and the DOJ;
 - (7) Recommend personnel actions for subordinates in accordance with Office of Personnel Management (OPM) regulations and the OIG's personnel management program before final authorization by the DAIG/E&I;
 - (8) Certify time and attendance reports and biweekly time sheets for all subordinates;
 - (9) Authorize and approve changes in full-time work schedules (including Alternate Work Schedules (AWS) and telework) for all subordinates subject to the OIG and the Division's policies;
 - (10) Approve requests for overtime pay and overtime as compensatory time earned, subject to the OIG and Division's overtime or compensatory policies and budgetary constraints, before final authorization by the DAIG/E&I;
 - (11) Approve requests for travel compensatory time for all subordinates subject to the OIG and Division's compensatory time earned policies;
 - (12) Recommend and approve non-foreign travel and all travel related documents, including travel authorizations and advances, for official travel for subordinates subject to the OIG's travel regulations and the Division's travel policies;
 - (13) Recommend and approve Individual Development Plans for all subordinates with training focused on core skill levels identified essential for OIG Inspectors and on strengthening staff knowledge of the Department's programs and operations before final authorization by the DAIG/E&I; and
 - (14) Approve training request for all subordinates in accordance with the Division's training plan before final authorization by the DAIG/E&I.
- B. Authorities Retained by the Administrative Officer. The Administrative Officer in the E&I Division is delegated the following responsibilities and functions to:
- (1) Certify that invoices are correct, legal, and proper for payment;
 - (2) Serve as E&I's Contract Officer's Technical Representative;
 - (3) Track and document E&I's implementation of operational and administrative program goals, policies, procedures, and performance;
 - (4) Formulate and justify E&I's annual budget;

- (5) Determine availability of funds for all requisitions, awards, overtime pay, training, and other funded areas to ensure that they are in line with the approved operating plan for the Division;
 - (6) Approve emergency supply and material purchases needed by staff personnel during the absence of senior management of \$3,000 or less;
 - (7) Recommend and approve Individual Development Plans and training requests for administrative support staff and student hires before final authorization by the DAIG/E&I;
 - (8) Approve time-sensitive training requests for all Division personnel, with the exception of training forms for the AIG/E&I and DAIG/E&I, during the absence of senior management;
 - (9) Recommend personnel actions in accordance with Office of Personnel Management regulations and the OIG's personnel management program for administrative support staff and student hires before final authorization by the DAIG/E&I;
 - (10) Approve requests for overtime pay and overtime as compensatory time earned for administrative staff and students, subject to the OIG and Division's overtime or compensatory policies and budgetary constraints, before final authorization by the DAIG/E&I;
 - (11) Initiate, develop, and maintain E&I's policies and procedures for administrative matters;
 - (12) Serve as the Accountable Property Officer;
 - (13) Serve as the Security Officer; and
 - (14) Serve as the system administrator for E&I databases.
- C. Authorities Retained by the Writer-Editor. The Writer-Editor in the E&I Division is delegated the following responsibilities and functions to:
- (1) Review all E&I work products to ensure these are clear, well-written, and comply with relevant standards; and
 - (2) Serve as the Intranet content manager for E&I.

003.6 Continuity of Operations. In the event of the simultaneous absence of the AIG/E&I and DAIG/E&I from the office, the AIG/E&I or DAIG/E&I, acting in the AIG/E&I's behalf, will designate in writing an Acting AIG/E&I.

- 270.1 Policy. It is the policy of the Office of the Inspector General (OIG) to provide for the effective and timely evaluation of employee performance. Performance standards will be consistent with Department of Justice (DOJ) Strategic Goals and Objectives, Chapter III, *Supporting the Mission: Efficiency and Integrity in the Department of Justice*.
- A. Organizational and performance goals will be communicated at every level of the OIG's workforce.
 - B. Individual performance management will be integrated directly with other critical performance measurement initiatives of the OIG. Performance standards will include critical elements that are results-focused and align with the OIG's, DOJ's, and the Human Capital strategic plans.
 - C. Supervisors, managers, and employees are required to receive periodic training on the OIG's performance management system.
 - D. Performance will be evaluated and improved where necessary, and the results of performance management will be used as a basis for appropriate personnel actions.
 - E. All participants in the process will be held accountable for accomplishing their performance management responsibilities.
- 270.2 References. This chapter is issued pursuant to 5 USC, Chapter 43, Subpart B; 5 CFR Part 430; and DOJ Order 1200.1, Part 2.
- 270.3 Scope. All OIG employees are covered by the provisions of this chapter, except for the following:
- A. Presidential Appointees;
 - B. Senior Executive Service employees;
 - C. positions filled by non-career Executive Assignments;
 - D. employees in positions for whom employment is intermittent or is not reasonably expected to exceed 120 calendar days in a consecutive 12 month period; and
 - E. employees in positions specifically excluded by law or regulation, e.g. students.
- 270.4 Responsibilities.
- A. The Inspector General (IG) will:
 - (1) ensure the proper administration of the performance management plan; and
 - (2) approve all subsequent revisions to the plan.
 - B. The Human Resources Officer (HRO) will:

- (1) implement the provisions of this chapter;
 - (2) provide for the issuance of guidelines, instructions, and training on the performance management program for supervisors and employees;
 - (3) provide technical assistance to OIG managers and supervisors regarding the performance management program; and
 - (4) consult with supervisors to develop plans to address unacceptable performance.
- C. Reviewing Officials, who are the direct supervisors to the rating official, will:
- (1) review and approve the content of Performance Work Plans and Performance Goals and Measures (hereafter referred to as PWP) and the assignment of ratings before ratings are discussed with employees;
 - (2) ensure ratings are appropriate and reflect employee performance;
 - (3) concur by signature on PWPs and any subsequent changes to the PWP; and
 - (4) concur by signature on the annual performance rating.
- D. Rating Officials, who are the first line supervisors to the employee, will:
- (1) involve the employee in developing a PWP and obtain the reviewing official's approval of the PWP;
 - (2) conduct at least one formal face-to-face progress review during the appraisal period; and
 - (3) prepare the final rating at the end of the performance appraisal period.
- 270.5 Performance Appraisal Period. The performance appraisal period for all covered employees will be October 1 through September 30. The minimum appraisal period is 90 days. The PWP must have been established for a minimum of 90 days before a rating is assigned.
- A. If an employee has not been under a PWP for the minimum 90-day period, the appraisal period may be extended until such time as the 90-day requirement is met.
 - B. The appraisal period may be extended if there is a change in an employee's first line supervisor within the 90-day period preceding the end of the rating cycle. If possible, the new supervisor should obtain input from the previous supervisor concerning the employee's performance for the period prior to the change.
 - C. The appraisal period may be extended up to 90 days based on the extended absence of the supervisor or the employee.

- D. Ratings of record should be completed within 60 days after the close of the rating period.

270.6 Performance Rating System. The OIG uses a four-level performance management system for appraising performance of all covered employees, with the following levels: Outstanding, Excellent, Successful, and Unacceptable (5 CFR § 430.208 – Pattern E).

If at any time during the appraisal period an employee’s performance falls to the Unacceptable level, the supervisor must contact and consult with the HRO for guidance. The HRO will consult with the Office of General Counsel as appropriate.

270.7 Performance Work Plans. A PWP is required and should be communicated to each covered employee within 30 days of the beginning of the appraisal period. The PWP will remain in effect through subsequent rating periods unless the employee is assigned substantially different duties. A new or revised PWP shall be issued within 30 days of the beginning of the change in duties. PWP’s should be communicated to new employees within 30 days of entering on duty with the OIG.

- A. The rating official must use the OIG Performance Appraisal Record, OIG Form V-270/1 (Revised) to document element and overall ratings. For managers and supervisors, the rating official must use the OIG Manager/Supervisor Performance Appraisal Record, OIG Form V-270/2 (Revised).
- B. The PWP should have a minimum of three critical performance elements tailored specifically to the major tasks listed in the employee’s position description and aligned with the goals and mission of the OIG and the DOJ Strategic Plan.
- C. The rating official should obtain input from the employee and the concurrence of the reviewing official prior to formally establishing the PWP. The individual element ratings will be used to generate the annual performance rating.
- D. PWP’s for certain groups of positions may be required to have mandatory critical elements that will not be subject to the limitations set in 270.7(B).
- (1) All PWP’s for managers and supervisors must include a critical element(s) addressing Human Capital management responsibilities, including the development of PWP’s and ratings; Equal Employment Opportunity; and the responsibilities imposed by OMB Circular A-123 (waste, fraud, and abuse).
- (2) The IG may direct the inclusion of a specific critical element related to an OIG-wide initiative, priority, or special project for any given appraisal cycle.
- E. Performance elements and standards must tie to organizational goals and the DOJ Strategic Plan and must be in concert with the human capital objectives of the OIG. All performance levels, except “Unacceptable,” will have defined standards that establish expectations in terms of the quality, quantity, and timeliness of work.
- F. PWP’s must contain results-focused elements to show that employees are held

accountable for achieving results from tasks performed.

- G. PWPs for supervisors, managers, and employees must contain critical elements with performance measures that focus on the customer and employee perspective.
- H. Performance standards must be written in a manner that makes meaningful distinctions about employees' performance. The "Outstanding" level should clearly, completely, and unequivocally define an unusually high level of performance that clearly is beyond normal management expectations.
- I. PWPs for supervisors and managers will contain a performance measure under the critical element "Accountability for Human Resources, Communication, and Professional Development" to account for rigorous performance management of subordinates and the alignment of subordinate plans with organizational goals.
- J. The rating official must obtain the approval of the reviewing official prior to communicating the final PWP to the employee. Any subsequent revisions or changes to the PWP must be reviewed and approved by the reviewing official prior to issuing the work plan to the employee.

270.8 Progress Reviews. The rating official must conduct at least one formal face-to-face progress review during the rating cycle. The rating official is encouraged to conduct more than one progress review so that the employee is aware of how he or she is performing in relationship to the PWP for his or her position.

- A. The employee's performance relative to the standards and each critical performance element, including any deficiencies in the employee's performance, will be discussed.
- B. The employee and rating official will each sign and date the employee's appraisal form to document the completion of the formal progress review.
- C. The progress review is not a formal determination of the employee's overall performance, and therefore cannot be grieved by the employee.

270.9 Annual Performance Appraisal. The rating official must maintain an awareness of the performance of the employee throughout the appraisal cycle to ensure timely delivery of a completed, approved, formal appraisal of the employee's performance for the rating period.

- A. Appraising Performance in Special Circumstances.
 - (1) Details or temporary promotions. For employees detailed for 120 days or more, the detail supervisor must prepare a PWP composed of no less than one critical element, and must prepare an interim rating at the conclusion of the detail period. The interim rating will be considered by the rating official in arriving at an overall rating. For details or temporary assignments of less than 120 days, the detail supervisor may submit narrative comments to the rating official for consideration.

- (2) Transfers. Rating officials are required to furnish or accept a summary performance rating when an employee transfers out or transfers in to the same type of work and consider that rating in deriving the rating of record.
 - (3) Reassignments. An interim rating must be prepared at the time there is a substantive change in the employee's position within an office or division or the employee moves to a position in the same type of work outside of the office or division, provided the employee has been under performance standards for the minimum 90-day rating period. This rating is to be considered by the rating official at the end of the cycle.
- B. Assignment and Documentation of Rating Levels. The rating official must use the OIG Performance Appraisal Record, OIG Form V-270/1 (Revised) to document elements, standards, and overall ratings. The form is available on the OIG intranet.
- (1) Performance Element Ratings. At the end of the appraisal cycle, the rating official will evaluate actual employee performance in comparison with defined standards for each critical performance element and assign one of the following rating levels:
 - a. "Outstanding" – The employee's performance at this level is consistently exceptional, far exceeds what is normally required of the job, and is deserving of special recognition.
 - b. "Excellent" – The employee's performance markedly and consistently exceeds the performance expectations for successful performance.
 - c. "Successful" – The employee's performance satisfies the established performance standards for acceptable performance.
 - d. "Unacceptable" – The employee's performance falls below the established standards for successful performance. The rating official must provide a written narrative summarizing performance deficiencies in the remarks section provided on the form. The rating and/or reviewing official must contact the HRO prior to assigning any employee an Unacceptable rating.

The rating official must provide the employee an opportunity to voluntarily submit a self-assessment of his or her performance achievements during the performance rating process. These comments are to be considered by the rating official prior to assigning element ratings.

The rating official will take into account the employee's performance strengths and weaknesses, and make a summary judgment of the level that best represents the employee's performance as a whole compared to the defined performance standards.

- (2) Documentation of Individual Element Ratings. Written narrative assessments must be provided for each individual element rating. Narrative assessments must be recorded on the Performance Appraisal Record for Progress Review,

OIG Form V-270/1A.

- C. Determination and Documentation of Summary Overall Rating. The rating official should provide a summary narrative assessing the employee's overall performance and contribution to achieving the goals and objectives of the organization during the rating period.

The PWP's for OIG staff consist of a minimum of three critical elements and are assigned the following weight factors:

Element 1, "Accountability for Organizational Results," accounts for 60 percent of the overall rating;

Element 2, "Accountability for Human Resources, Communication, and Professional Development," accounts for 20 percent of the overall rating; and

Element 3, "Accountability for Taxpayer Value and Customer Service," accounts for 20 percent of the overall rating.

The overall rating for the performance rating period will be derived as follows:

- a. Outstanding – Performance is rated Outstanding in Elements 1, 2, and 3; or Performance is rated Outstanding in Element 1 *and* Elements 2 and 3 are either Excellent or Outstanding.
- b. Excellent – Performance is rated Outstanding in Element 1 *and* Elements 2 and 3 are rated no lower than Successful but are not both Excellent; or Performance is rated Excellent in Elements 1, 2, and 3; or Performance is rated Excellent *and* Elements 2 and 3 are no lower than Successful. (If Element 1 is rated as Excellent and one of or both Elements 2 and 3 are rated Outstanding, the overall rating may *not* be rated Outstanding and may *not* be rated below Excellent.)
- c. Successful – Performance rated Successful in Elements 1, 2, and 3; or Performance is rated Successful in Element 1 *and* one of or both Elements 2 and 3 are rated at either Outstanding or Excellent.
- d. Unacceptable – Performance in one or more of the three Elements fails to meet standards for successful performance.

The overall ratings resulting from combinations of individual element ratings are depicted in the following table. (Element 1 rating is in **bold**):

Overall Ratings

Outstanding	Excellent	Successful	Unacceptable
O O O	O E S	S O O	At least one U
O O E	O S E	S O E	
O E O	O S O	S E O	
O E E	O O S	S O S	
	O S S	S S O	
	E O O	S E E	
	E O E	S E S	
	E E O	S S E	
	E O S	S S S	
	E S O		
	E E E		
	E E S		
	E S E		
	E S S		

- D. Approval by Reviewing Official. A completed rating of record must be reviewed and approved by the reviewing official before is it communicated to the employee. The reviewing official's determination of an element or overall rating may override that of the rating official.

270.10 Actions Based on Performance Ratings.

- A. Award Recognition. Performance rated Excellent or Outstanding may be recognized through appropriate recognition or incentive awards consistent with IG Manual, Volume V, Chapter 250, Awards. Rating or reviewing officials may submit or cite to Part E of V-270/2 to satisfy the justification requirement for award nominations.
- B. Actions Based on Overall Rating of "Unacceptable." Any employee, including supervisors and managers, who receives an overall rating of "Unacceptable" at any time during the appraisal cycle may be reassigned, reduced in grade, or removed from federal service in accordance with applicable personnel procedures. In addition, any employee with a current rating of "Unacceptable" will not be granted a Within Grade Increase. Supervisors must contact the HRO if an employee's performance has reached the Unacceptable level, and are encouraged to contact the HRO as soon as it appears that an employee's performance may be approaching the Unacceptable level.
- (1) The opportunity period may be no less than 30 calendar days. During this period an employee will be provided assistance, e.g., training or counseling, to improve their unacceptable performance.

- (2) Any administrative action already initiated under the OIG's previously approved appraisal program shall continue to be processed in accordance with that program and with 5 USC 4303.
- C. Performance Improvement Plans. In most instances, before any personnel action is taken against an employee whose performance has become unacceptable, the employee will be placed on a Performance Improvement Plan (PIP) for no less than a 30-day period. A PIP informs the employee in writing of the critical elements in which he or she is failing, what is needed to bring performance up to an acceptable level, what assistance will be provided (such as training or counseling), and the consequences of failing to improve during the opportunity period. Managers should consult with the HRO and the Office of General Counsel before drafting a PIP.
- D. Employee Challenges of Performance Ratings. The employee may challenge a performance rating through the IG Manual, Volume V, Chapter 290, Grievance Procedures. Progress reviews and the establishment of the PWP are excluded from coverage under the OIG grievance procedure. The employee should contact DOJ's Equal Employment Opportunity Staff on challenges that involve allegations of discrimination subject to the coverage of equal employment opportunity statutes and regulations.
- 270.11 Performance Management Records. In accordance with Title 5 C.F.R. 293.404, the OHR will maintain all finalized, original Performance Appraisal Records in Employee Performance Files for a period of no less than four years. All performance forms, including the Performance Appraisal Record Form V-270/1(Revised), documents generated to record progress reviews, and interim and final ratings will be filed in the Employee Performances Files. If an employee transfers to another government agency, the Employee Performance File ratings will be forwarded to the gaining agency.
- 270.12 Program Evaluation. The Performance Management Program will be continuously monitored and revised as necessary.
- 270.13 Program Changes and Revisions. This plan has been approved by the Justice Management Division (JMD) and the Office of Attorney Recruitment and Management (OARM). Subsequent changes to the plan must be submitted to JMD and OARM for approval prior to implementation.

INSPECTOR GENERAL MANUAL
Volume V. Chapter 270, Performance Management
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume 1, Chapter 001, Directives Management System.

As of 2004, the Performance Appraisal System was changed from a Pass/Fail appraisal program to a 4-level system and therefore the revised directive for this chapter has been completely rewritten and replaces the current directive on file.

270.7 A Instruction regarding the form V-270/2 was added.

- 295.1 Purpose. This Chapter supplements provisions of Department Order 1752.1A, Discipline and Adverse Actions.
- 295.2 Scope. Department Order 1752.1A is applicable to all employees of the OIG. Provisions of this chapter supplement and clarify the Order. This chapter is applicable to all employees of the Office of the Inspector General.
- 295.3 Authority. These procedures are in accordance with 5 CFR Parts 550, 735 and 752 and in accordance with and/or supplements Department Orders 1551.4A and 1752.1A.
- 295.4 Policy. OIG employees are expected to maintain high standards of honesty, integrity and conduct to assure the effective accomplishment of the OIG mission and the continued confidence of the Department and the public.
- 295.5 Definitions.
- A. Adverse Actions. A suspension, reduction in grade or pay, or removal effected in accordance with 5 CFR Part 752.
 - B. Major Adverse Action. A disciplinary adverse action appealable to the Merit Systems Protection Board (MSPB), i.e. a suspension of 15 calendar days or longer, a reduction in grade or pay, or a removal.
 - C. Office Heads. Special Agents in Charge, Regional Audit Managers, Directors, ADP & Financial Statement, Office of Operations and Office of Policy and Planning of the Audit Division, the General Counsel, the Director of the Internal Control Unit, the Directors, Management, Planning, and Review and Field Operations of the Inspections Division and the supervisors one level below the Deputy Assistant Inspectors General of the Management and Planning Division.
- 295.6 Responsibilities.
- A. The Inspector General:
Makes final decisions on notices of proposed adverse action issued by the Inspector General or the Deputy Inspector General, except for those involving attorneys.
 - B. The Deputy Inspector General:
 - (1) Makes final decisions on notices of proposed adverse action issued by the Assistant Inspectors General;
 - (2) Proposes adverse actions for Assistant Inspectors General;
 - (3) Issues written reprimands to attorneys of the Office; and
 - (4) Supervises the investigation and prepares memoranda recommending adverse actions against attorneys for a decision by the Deputy Attorney General.

- C. The Assistant Inspectors General:
- (1) Make final decisions on adverse actions proposed by Deputy Assistant Inspectors General or office heads;
 - (2) Propose adverse actions for Deputy Assistant Inspectors General;
 - (3) Place employees on home duty status pending the result of an investigation of alleged serious disciplinary offenses; and
 - (4) Ensure that individual cases are processed within a reasonable time and that discipline is applied fairly and uniformly throughout the Division.
- D. The Assistant Inspector General, Management and Planning Division also:
- (1) Is responsible for the administration of this chapter;
 - (2) Has the authority to post audit and correct any adverse action taken in the Office; and
 - (3) Will provide for training of supervisors on their responsibilities under this chapter, as needed.
- E. The Deputy Assistant Inspectors General:
- (1) Make final decisions on adverse actions proposed by the office heads in the Division, if designated by the AIG;
 - (2) Propose adverse actions for office heads;
 - (3) Place employees on home duty status pending the result of an investigation of alleged serious disciplinary offenses, if designated by the AIG; and
 - (4) Ensure that supervisors are knowledgeable of their responsibilities under this chapter.
- F. Office Heads.
- (1) Propose major adverse actions for employees in their office; and
 - (2) Make final decisions on non-major adverse actions for employees proposed by supervisors.
- G. General Counsel represents the Office in matters that fall within the jurisdiction of the MSPB or the Office of Special Counsel.
- H. Personnel Officer:
- (1) Provides advice and assistance to management on the coverage and application of this chapter;

- (2) Ensures that employees are advised of their rights under this chapter;
- (3) Ensures that individual cases are processed within a reasonable time;
- (4) Ensures that each new employee is provided with a copy of the Standard Schedule of Disciplinary Offenses and Penalties; and
- (5) Maintains the case records of disciplinary and adverse actions in the OIG except those designated as litigation files which are maintained by the General Counsel.

- I. Supervisors and Managers administer work force discipline by taking or proposing disciplinary actions when they have the authority and refer serious matters beyond their authority to the proper officials.
- J. Employees are responsible for complying with written standards of conduct and for refraining from any activity which could compromise the high standards of honesty, integrity and conduct expected of OIG employees.

295.7 Authority to Propose and/or Decide Disciplinary Actions.

A. General.

- (1) Authority to take adverse actions and issue reprimands should be at the lowest appropriate managerial level.
- (2) Supervisors and managers are encouraged to contact the Personnel Officer and staff when employee conduct or performance first becomes an issue so that an appropriate approach to the problem can be developed.
- (3) Officials who make decisions on adverse actions will take into consideration the Department's Standard Schedule of Disciplinary Offenses and Penalties [Appendix A and B], and the circumstances of both the case and the individual when determining the appropriate penalty to impose.
- (4) The official who makes final decisions on adverse actions must be an official who will assure an impartial decision, i.e. an official who has not been personally involved in a case.
- (5) If the IG was personally involved in the circumstances of a case, the IG has the option of being the official who decides the case or designating another Department official (non-OIG) to serve as the official who decides the case.

B. Official Reprimands should be issued by the immediate supervisor of the employee.

C. Suspensions of 14 days or less will be proposed by the immediate supervisor or a higher level official. The final decision on these proposed adverse actions must be decided by an official no lower than an office head.

D. Major Adverse Actions will be proposed by the office head or higher level official. The final decision on these proposed adverse actions must be decided by an official no

lower than a Deputy Assistant Inspector General.

E. Adverse Actions for Attorneys will be handled in accordance with the Attorney Personnel Memorandum 91-10, Procedures Governing Adverse Actions Against Attorneys.

- (1) The Deputy Inspector General will propose all adverse actions for attorneys in the OIG.
- (2) The Deputy Attorney General makes all decisions on adverse actions for attorneys of the OIG.

295.8 Review of Actions. Prior to their issuance, all proposals to take disciplinary or adverse action and all final decisions on disciplinary or adverse action will be forwarded to the Personnel Officer for review to ensure consistency with statute, Department regulations and internal policies of the OIG.

295.9 Maintenance of Case Records. Case records of disciplinary and adverse actions will be established and maintained by the Personnel Officer. Litigation files are maintained by the General Counsel.

295.10 Home Duty Status. Employees under certain conditions may have their duty station changed to their home for a period of time.

A. Conditions. An employee may be assigned to home duty when the employee:

- (1) is under investigation or under notice of proposed disciplinary action for conduct which may have been a serious breach of security, or serious breach of integrity of the OIG or may have endangered other employees at the work place; or
- (2) is a danger to himself or others.

B. Authority. The Assistant Inspectors General [or the Deputy Assistant Inspectors General, if designated by the AIG], the General Counsel, and the Director of the Internal Control Unit may place an employee in their Division or unit on home duty status pending the outcome of an investigation. This duty status is similar to "stand-by duty" or "on-call status," as described in 5 CFR 550.431.

C. Activity. During normal working hours, the employee must be ready and available for work as if the employee was at the work place.

- (1) An employee on home duty status must be readily available over the phone during normal working hours.
- (2) Work that can be done at home may be assigned to the employee. The employee may come to the office to receive work or the supervisor may go to the employee's home and deliver work.
- (3) During normal working hours, the employee must be ready and able to report to the work place when so ordered.

- (4) Home duty status does not qualify an employee for Administratively Uncontrollable Overtime in accordance with DOJ Order 1551.4A, Section 8.

INSPECTOR GENERAL MANUAL
Volume V, Chapter 295
Discipline and Adverse Actions
Revisions

This chapter was originally issued on December 31, 1991. It was partially updated on July 25, 2016, and June 29, 2017.

This chapter was partially updated on July 25, 2016, to include the following changes:

Appendix A. Combined Appendix A, “Standard Schedule of Disciplinary Offenses and Penalties” with Appendix B, “OIG Supplement.”

Appendix A. Added the language: “Failure to adhere to or violation of DOJ OIG Information Technology Policy.”

This chapter was partially updated on June 29, 2017, to include the following changes:

Appendix A: Added items 34-47

APPENDIX A

**DOJ Standard Schedule of Disciplinary Offenses and Penalties
with OIG Supplements**

	NATURE OF OFFENSE	EXPLANATION	FIRST OFFENSE	SECOND OFFENSE	THIRD OFFENSE	RECKONING PERIOD
1.	Failure to adhere to or violation of DOJ OIG Information Technology Policy.		Official reprimand to removal.	Official reprimand to removal.	Official reprimand to removal.	2 yrs.
2.	Unexcused or unauthorized absence of 8 hours or less.	Unauthorized absence of 8 hours or less, tardiness, leaving the job without permission.	Official reprimand to 1-day suspension.	Official reprimand to 5-day suspension.	Official reprimand to removal.	6 mos.
3.	Unexcused or unauthorized absence of between 1 and 5 consecutive workdays.	Unauthorized absence of 8 to 40 hours.	1-day to 5-day suspension.	5-day suspension to 15-day suspension.	15-day suspension to removal.	1 yr.
4.	Excessive unauthorized absence	Unauthorized absence of more than 5 consecutive workdays.	5-day suspension to removal.	15-day suspension to removal.	Removal	2 yrs.
5.	Careless workmanship or negligence resulting in spoilage or waste of materials or delay in work production.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
6.	Failure or delay in carrying out orders, work assignments, or instructions of superiors.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
7.	Failure to honor just debts without good cause.	A just financial obligation is one acknowledged by the employee, reduced to judgment by a court or imposed by law.	Official reprimand.	Official reprimand.	Reprimand to removal.	2 yrs.
8.	Loafing, wasting time, sleeping on the job, or in-attention to duty.	Potential danger to safety of persons and/or actual damage to property is a consideration in determining severity of the penalty, as is potential or actual adverse impact on government operations.	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
9.	Disobedience to constituted authorities, or refusal to carry out a proper order from any supervisor or other official having responsibility for the work of the employee; insubordination.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
10.	Failure to observe: (1) precautions for personal safety;		Official reprimand to	15-day suspension to	Removal.	2 yrs.

	(2) posted rules; (3) signs; (4) written or oral safety instructions, or failure to use protective clothing or equipment.		removal.	removal.		
11.	Unauthorized possession of, use of, loss of, or damage to, Gov't property or property of others including a U.S. Gov't owned motor vehicle, aircraft or boat.	Use of U.S. Gov't owned motor vehicle, aircraft or boat for other than official U.S. Gov't business (including comingling of personal or official business) is UNAUTHORIZED USE and is NOT considered a misuse. (NOTE: 31 U.S.C. Section 638 provides a MINIMUM of 30-day suspension for willful use or authorization for use of other than official purposes. Willful use is (a) intentional unauthorized use with or without illegal intent; or (b) careless or intentional disregard or plain indifference to statutory or regulatory requirements.	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
12.	Gambling or unlawful betting on Government owned or leased premises.		Official reprimand to 10-day suspension.	10-day suspension to removal.	15-day suspension to removal.	2 yrs.
13.	Promotion of gambling on Gov't owned or leased premises.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
14.	Malicious damage to Government property to the property of others.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
15.	Endangering the safety of or causing injury to personnel through carelessness or failure to follow instructions.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
16.	Theft or attempted theft or misappropriation of Gov't property or the property of others.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
17.	Conversion of Gov't funds to personal use.	Includes, but is not limited to, travel advances, imprest funds, or amounts received as collections.	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
18.	Disorderly conduct, fighting, threatening, or attempting to inflict bodily injury to another, engaging in dangerous horseplay.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
19.	Disrespectful conduct; use of insulting, abusive or obscene language to or about others.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.

20.	Refusal to cooperate in any official U.S. Gov't inquiry or investigation, including a refusal to answer work related questions or attempting to influence others involved in the inquiry.	Includes administrative or criminal investigation, grievance inquiry, EEO investigation, and any other administrative inquiry.	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
21.	Reporting for duty or being on duty under the influence of intoxicants or other drugs; unauthorized possession of intoxicants or drugs on Government owned or leased premises.		Official reprimand to removal.	15-day suspension to removal.	30-day suspension to removal.	2 yrs.
22.	Criminal, dishonest, infamous, or notoriously disgraceful conduct.	On or off duty	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
23.	Falsification, misstatement, exaggeration or concealment of material fact in connection with employment, promotion, travel voucher, any record, investigation or other proper proceeding.	Includes but is not limited to, the destruction of records to conceal facts, and a concealed conflict of interest in the performance of official duties.	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
24.	Discrimination in official action against an employee or applicant because of race, religion, sex, national origin, age, handicapping condition, or any reprisal action taken against an employee for filing a discrimination complaint, grievance, or complain with the Special Counsel, MSPB.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
25.	Use of Department of Justice identification for other than official U.S. Government business.	Example: use to coerce, intimidate or deceive (Includes ID cards, badges, various bureau credentials and badges).	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
26.	Receiving or soliciting gifts, favors, or bribes in connection with official duties.		Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
27.	Intentional violation of rules governing searches and seizures.	Example: false statements in obtaining warrants, disregard of warrant requirements.	Official reprimand to removal.	15-day suspension to removal.	Removal.	2 yrs.
28.	Reckless disregard of rules governing searches and seizures.	Example: gross errors in obtaining warrants when standard procedure is to check further and there is time to check further.	Official reprimand to removal.	15-day suspension to removal.	Removal.	1 yr.
29.	Negligent violations of rules governing searches and seizures.	Example: executing warrant at wrong address, failing to check names of suspects.	Official reprimand to 1-day suspension.	Official reprimand to 5-day suspension.	Official reprimand to removal.	1 yr.
30.	A negligent action which violates any procedure contained in	Example: Repeated discrepancies in the	Official reprimand	Official reprimand to 5-day	5-day suspension to removal	2 yrs.

	Chapter 220 - <u>Document Security</u> .	marking and handling of classified materials		suspension		
31.	An intentional action which seriously violates any procedure contained in Chapter 220 - <u>Document Security</u> .	Example: Intentionally allowing classified documents to be viewed or put into the possession of individuals who do not have appropriate security clearance.	Official reprimand to removal	15-day suspension to removal	Removal	2 yrs.
32.	Violations of the Department Standards of Conduct or compromise of the high standards of honesty, integrity and conduct expected of OIG employees	Example: Participating in an investigation in which the employee has a personal, financial or political relationship with individuals under investigation.	Official reprimand to removal	15-day suspension to removal	Removal	2 yrs.
33.	Careless handling of OIG credentials leading to loss.		Letter of Caution	Official reprimand	5-day suspension	2 yrs.
34.	Misuse of agency purchase card and travel card		Reprimand to Removal	Removal		
35.	Use of OIG Internet and/or OIG system to access, seek, review, download, transmit, and/or store sexually explicit material		Removal			
36.	Failure to immediately report an actual or suspected information security breach (i.e., PII or National Security)		Reprimand to 5-day suspension	14-day suspension to removal	Removal	
37.	Violations of security procedures covering information, documents, records, or other material classified or sensitive to the Government, including Privacy Act protected records		Reprimand to 14-day suspension	15-day suspension to removal	Removal	
38.	Unauthorized disclosure of information, documents, records, or other material classified or sensitive to the Government, including Privacy Act protected records.		Reprimand to removal	15-day suspension to removal	Removal	
39.	Unauthorized access, or providing unauthorized access, to classified or Law Enforcement sensitive systems or information.		Reprimand to 14-day suspension	15-day suspension to removal	Removal	
40.	Violation of traffic regulations, reckless driving, or improper operation of a vehicle on Government-controlled premises.		Reprimand to 14-day suspension	15-day suspension to removal	Removal	
41.	Unauthorized canvassing, soliciting, or peddling at DOJ or		Reprimand to 1 - day suspension	2-day suspension to 14-day	Removal	

	OIG worksite or while on-duty			suspension		
42.	Failure to honor just debts or legal obligations in a timely manner.		Reprimand to 14-day suspension	15-day suspension to removal	Removal	
43.	Engaging in political activity that violates the Hatch Act		30-day suspension to removal	30-day suspension to removal	30-day suspension to removal	
44.	Interfering with employees' rights, or taking reprisal against employees for exercising their rights, to file or participate in a grievance or appeal.		Reprimand to 14-day suspension	15-day suspension to removal	Removal	
45.	Ethics violation not elsewhere covered in this Table.		Reprimand to removal	5-day suspension to removal	14-day suspension to removal	
46.	Committing a prohibited personnel practice not elsewhere covered in this Table.		Reprimand to removal	5-day suspension to removal	14-day suspension to removal	
47.	Engaging in conduct determined to constitute sexual harassment		Reprimand to removal	5-day suspension to removal	14-day suspension to removal	

- 101.1 Policy. The Office of the Inspector General (OIG) shall maintain an effective system of internal accountability and control.
- 101.2 Reference. This chapter is issued pursuant to the authority contained in:
- A. Federal Managers' Financial Integrity Act of 1982 (Integrity Act), P.L. 97-225, 31 U.S.C. 3511 (1983).
 - B. OMB Circular A-123 (Revised), Management Accountability and Control, December 21, 2004.
 - C. DOJ Order 2860.3B, Federal Managers' Financial Integrity Act of 1982, July 15, 1996.
- 101.3 Scope. Provisions of this chapter apply to all OIG personnel.
- 101.4 Responsibilities. The responsibilities of OIG staff are established as follows:
- A. The Inspector General (IG) ensures the development, maintenance, and evaluation of the OIG internal control system, and provides the Attorney General annually with written assurance that the internal controls implemented in the OIG are in conformance with all established requirements.
 - B. The Internal Control Officer, Management and Planning Division, oversees, monitors, and follows up on the implementation of the management control process. This includes the provision of assurances to the IG that these processes were conducted in a thorough and conscientious manner in accordance with all established requirements.
 - C. The Internal Control Coordinator plans and coordinates management control activities for the OIG.
 - D. The Internal Oversight Officials oversee the management control process for their areas of responsibility.
 - E. The Assessable Unit Managers assess whether management controls are in place and working for those operations, functions, and activities within the unit for which they are responsible.
 - F. OIG Managers ensure the quality and timeliness of program performance, increase productivity, control costs, mitigate adverse aspects of OIG operations, and manage programs with integrity and in compliance with applicable law. OIG managers identify program improvements and take timely and effective action to correct deficiencies.
- 101.5 Procedures.
- A. The IG designates responsible officials in each division and the Immediate Office to oversee the management accountability and control process within their areas of responsibility. The IG also designates an Internal Control Officer, responsible for oversight of the OIG internal control process.

- B. All management accountability and control systems and processes are integrated and consolidated as a part of the OIG's routine methods of management and operations, rather than separate processes.
- C. The OIG uses management accountability and control systems--organization, policies, and procedures--to reasonably ensure that:
 - (1) programs achieve their intended results;
 - (2) resources are used consistent with the OIG's mission;
 - (3) programs and resources are protected from waste, fraud, and mismanagement;
 - (4) laws and regulations are followed; and
 - (5) reliable and timely information is obtained, maintained, reported and used for decision-making.
- D. The OIG divisions and the Immediate Office continually assess management controls and accountability using a variety of information sources. Examples of these include management reviews, peer reviews, performance indicator reports pursuant to the Government Performance and Results Act, and compliance reviews.
- E. The IG reports annually to the Attorney General on the status of the OIG management accountability and control systems. The divisions and the Immediate Office provide input for this report in response to a data call.

INSPECTOR GENERAL MANUAL
Volume V, Chapter 101
Internal Controls
Revisions

FORMAT: This chapter has been reformatted to conform to the structure as described in Volume I, Chapter 001, Directives Management System.

This directive is revised to incorporate the changes to OMB Circular A-123.

- 003.1 Policy. All redelegations state the authority, responsibilities, management, and staff of the Office of the Inspector General (OIG), Oversight and Review Division (O&R).
- 003.2 Reference.
- A. Inspector General Act of 1978 as amended;
 - B. Attorney General Order No. 1341-1989, Delegating Certain Authorities to the Inspector General, Department of Justice (April 14, 1989);
 - C. IGM, Volume I, Chapter 002, Mission, Organization, and Functions; and
 - D. IGM, Volume I, Chapter 003, Delegation of Authorities.
- 003.3 Scope. This chapter applies to O&R.
- 003.4 Procedures. When designated to act on behalf of the Assistant Inspector General for O&R (AIG/O&R), either of the two Deputies Assistant Inspector General for O&R (DAIG/O&R) or the Associate Deputy Assistant Inspector General for O&R (ADAIG/O&R) may exercise the full range of administrative and operational authorities described in Inspector General Manual (IGM) Volume I, Chapter 003, Delegation of Authorities, § 003.11.
- 003.5 Responsibilities.
- A. Authorities Retained by the DAIG/O&R. Authorities not specifically delegated in this chapter or elsewhere in IGM are retained by the AIG/O&R. The DAIG/O&R may be delegated with the following authorities:
 - (1) When authorized by the AIG/O&R, the Inspector General (IG), or the Deputy Inspector General (DIG), either of the two O&R DAIGs may serve as the AIG/O&R in the AIG/O&R's absence;
 - (2) Exercise signatory authority for the AIG/O&R, as appropriate;
 - (3) Provide legal advice and counsel on OIG law enforcement policies, procedures, and practices;
 - (4) Approve annual, sick, administrative, and other forms of leave for subordinates subject to leave policies and regulations of the OIG and Department of Justice (DOJ);
 - (5) Approve overtime and compensatory time for subordinates subject to the OIG's and DOJ's overtime and compensatory time regulations and procedures;
 - (6) Certify time and attendance reports for subordinate employees;

- (7) Approve miscellaneous purchases and claims for reimbursement (SF-1164);
 - (8) Approve travel authorizations, advances, and vouchers for official travel for subordinates subject to the OIG's and DOJ's travel regulations;
 - (9) Approve requisitions for goods and services in accordance with funding level authorities;
 - (10) Certify receipt of goods and services;
 - (11) Approve IG In\$tant awards;
 - (12) Authorize and approve training requests for subordinate employees; and
 - (13) Execute the following personnel actions in accordance with Office of Personnel Management procedures and the DOJ's merit staffing and personnel management system: (i) interview and recommend candidates from eligible applicants for appointment to vacant positions; (ii) recommend employees for promotion, within grade increases, reassignment, and awards; (iii) recommend or render disciplinary actions; (iv) initiate action for removal of an employee; (v) determine duties of subordinate employees; and (vi) conduct annual performance appraisals.
- B. Authorities Retained by the ADAIG/O&R. The ADAIG/O&R may be delegated with the following authorities:
- (1) When authorized by the AIG, the IG, or the DIG, the ADAIG/O&R may serve as the AIG/O&R in the AIG/O&R's and DAIG/O&R's absence;
 - (2) Exercise signatory authority for the AIG/O&R, as appropriate in the AIG/O&R's and DAIG/O&R's absence;
 - (3) Approve annual, sick, administrative, and other forms of leave for subordinates subject to leave policies and regulations of the OIG and DOJ;
 - (4) Approve overtime and compensatory time for subordinates subject to the OIG's and DOJ's overtime and compensatory time regulations and procedures;
 - (5) Certify time and attendance reports for subordinate employees;
 - (6) Approve miscellaneous purchases and claims for reimbursement (SF-1164);
 - (7) Approve travel authorizations, advances, and vouchers for official travel for subordinates subject to the OIG's and DOJ's travel regulations;
 - (8) Approve requisitions for goods and services in accordance with funding level authorities;

- (9) Certify receipt of goods and services;
- (10) Approve IG Instant awards;
- (11) Authorize and approve training requests for subordinate employees; and
- (12) Execute the following personnel actions in accordance with Office of Personnel Management procedures and the DOJ's merit staffing and personnel management system: (i) interview and recommend candidates from eligible applicants for appointment to vacant positions; (ii) recommend employees for promotion, within grade increases, reassignment, and awards; (iii) recommend or render disciplinary actions; (iv) initiate action for removal of an employee; (v) determine duties of subordinate employees; and (vi) conduct annual performance appraisals.

003.6 Continuity of Operations. In the event of the simultaneous absence of the AIG/O&R, DAIG/O&R, and ADAIG/O&R from the office, the AIG/O&R and DAIG/O&R, acting in the AIG/O&R's behalf, will designate in writing an Acting AIG/O&R.

Table of Contents

220.1	Policy	1
220.2	Reference	1
220.3	Scope.....	1
220.4	Responsibilities.....	1
	A. The Inspector General.....	1
	B. The Security Programs Manager	1
	C. Office Heads	1
	D. The Security Officer	1
	E. Employees.....	1
220.5	Classifying Documents and Materials	2
	A. Original Classification	2
	B. Derivative Classification	2
	C. Emergency Classification Actions.....	2
220.6	Dissemination of Information.....	2
	A. General.....	2
	B. Dissemination of Classified Documents and Materials.....	3
	C. Conferences and Meetings.....	3
	D. Access by Persons Outside the Executive Branch.....	4
220.7	Use of Classified Information in Judicial Proceedings.....	4
	A. General.....	4
	B. Proceedings.....	4
220.8	Receiving Documents and Materials	6
	A. General.....	6
	B. Accountability for Transmitted Documents and Materials	6
220.9	Security Containers.....	6
	A. General.....	6
	B. Standards.....	7
	C. Storage Requirements for Top Secret.....	7
	D. Storage Requirements for Secret	7
	E. Storage Requirements for Confidential	8
	F. Marking of Containers.....	8
	G. Combinations.....	8
	H. Check Sheets.....	9

220.10	Safeguarding Documents and Materials.....	9
A.	General.....	9
B.	Precautions.....	9
C.	Safeguards (b) (7)(E).....	10
D.	Safeguards (b) (7)(E).....	10
E.	Security Checks.....	10
220.11	Transmission by Courier.....	11
A.	Control.....	11
B.	Briefing.....	11
C.	Responsibilities.....	11
D.	(b) (7)(E).....	11
220.12	Transmission of Classified Materials.....	12
A.	(b) (7)(E).....	12
B.	13
C.	13
220.13	Reproduction of Classified Materials.....	13
A.	Control.....	13
B.	Restrictions.....	13
220.14	Disposing of Documents and Materials.....	14
A.	Methods of Destruction.....	14
B.	Approval.....	14
220.15	Reporting Requirements.....	14
A.	Daily Reports.....	14
B.	Security Violation Report.....	14
C.	Other Reports.....	15
220.16	Computer/ STE.....	15
A.	Computer Security.....	15
B.	Secure Telephone Equipment (STE).....	15

Chapter Title: Volume XXX - XXXX	Date:		
	Reply by:		
	Contact Person: Amy Reeder Phone Number: 202-616-4608		
Chapter Number:	Return to: Amy Reeder Directives Coordinator		
REVIEWING OFFICES:			
Reviewing Official: Check Appropriate Box <input type="checkbox"/> Deputy Inspector General <input type="checkbox"/> General Counsel <input type="checkbox"/> AIG – O&R <input type="checkbox"/> AIG – Audit <input type="checkbox"/> AIG – Investigations <input type="checkbox"/> AIG – Evaluation & Inspections <input type="checkbox"/> AIG – Management & Planning	Signature:	Date:	Concur: <input type="checkbox"/> Nonconcur: <input type="checkbox"/>
	NONRESPONSE BY CLOSE OF BUSINESS XX/XX/XXXX EQUATES TO CONCURRENCE		
Comments:			