BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-212

1 OCTOBER 1997

Communications and Information

REPORTING COMSEC INCIDENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/GCI (Ms Jean Alf)
Supersedes AFI 33-212, 20 March 1995

Certified by: HQ USAF/SCXX (Lt Col McGovern)
Pages: 30
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-2, *Information Protection*, and applicable parts of National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4003, *Reporting and Evaluating COMSEC Incidents.* It sets up procedures for reporting incidents affecting the security of communications security (COMSEC) material to the National Security Agency (NSA), the Air Force Communications Agency (AFCA), appointed controlling authorities, and other cognizant authorities in established chains of command. It applies to all Air Force military and civilian personnel and Air Force contractors who get COMSEC support from the Air Force. This publication pertains to all COMSEC material, including controlled cryptographic items (CCI), hard-copy key-in electronic forms, keyed common-fill devices, cryptographic equipment, and electronically generated keys (generated by field and electronic key management systems [EKMS]). The term major command (MAJCOM), when used in this publication, includes field operating agencies and direct reporting units. Submit technical questions and recommended changes through appropriate MAJCOM COMSEC channels to HQ AFCA/GCI, 203 West Losey Street, Room 2040, Scott AFB IL 62225-5234. Send messages to: HQ AFCA SCOTT AFB IL//GCI//. Refer recommended changes and conflicts between this and other publications to HQ AFCA/XPXP, 203 West Losey Street, Room 1060, Scott AFB IL 62225-5233, using AF Form 847, **Recommendation for Change of Publication.**

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Updates unit designators and office symbol changes. Adds charts for reporting incidents and practices dangerous to security (PDS).

1. Introduction:

1.1. Purpose. COMSEC incidents are reported so that appropriate officials can determine if the incidents have seriously affected the security of the cryptosystems involved or have the potential to do any harm to the security of the United States. Reporting COMSEC incidents also provides the basis for identifying trends in incident occurrences and for developing policies and procedures to prevent recurrence of similar incidents.

1.2. References and Terms. Terms and acronyms in Air Force Manual (AFMAN) 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary* (to be renamed *Information Protection Glossary* when current draft is published), apply to this publication. Key terms are listed below. Additional references, acronyms, and terms used in this AFI are explained in **Attachment 1**.

1.2.1. COMSEC Incident. Occurrence that potentially jeopardizes the security of COMSEC material or the secure electrical transmission of national security information.

1.2.2. COMSEC Insecurity. COMSEC incident that has been investigated, evaluated, and determined to jeopardize the security of COMSEC material or the secure transmission of information.

2. Types of Communications Security Incidents. Cryptographic, personnel, and physical COMSEC incidents are identified below. Additional reportable incidents unique to a particular cryptosystem or to an application of a cryptosystem, are normally listed in the AFI 33-2XX series, operating instructions, and maintenance manuals for that specific cryptosystem. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3260.01, (S) *Joint Policy Governing Positive Control Material and Devices* (U), contains a complete list of reportable incidents involving positive control material (PCM). **NOTE:** The reporting requirements in this section are exempt from licensing in accordance with paragraph 2.11.1 of AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and InterAgency Air Force Information Collections* (will convert to AFI 33-324.)

2.1. Cryptographic Incidents. Cryptographic incidents include equipment malfunction or operator error that adversely affect the cryptosecurity of a machine, auto-manual, or manual cryptosystem. Report cryptographic incidents by message (see Attachments 4 and 6). Examples are:

2.1.1. Using a COMSEC key that is compromised, superseded, defective, previously used (and not authorized for reuse), or incorrect application of keying material. Examples are:

2.1.1.1. Using keying material produced without the authorization of NSA (e.g., unauthorized maintenance or data encryption standard key, or locally contrived codes).

2.1.1.2. Using any keying material for other than its intended purpose without the authorization of NSA.

2.1.1.3. Unauthorized extension of a cryptoperiod.

2.1.2. Using COMSEC equipment with defective cryptographic logic circuitry, or using unapproved operating procedures. Examples include:

2.1.2.1. Plain-text transmission resulting from COMSEC equipment failure or malfunction.

2.1.2.2. Any transmission, during or after an uncorrected failure, that may cause improper operation of COMSEC equipment.

2.1.2.3. Using COMSEC equipment without completing a required alarm-check test or after failure of a required alarm-check test.

2.1.3. Using a cryptosystem not approved by NSA.

2.1.4. Discussing the details of a COMSEC equipment failure or malfunction on nonsecured telecommunications equipment.

2.1.5. Any other occurrence that may jeopardize the cryptosecurity of a COMSEC system.

2.2. Personnel Incidents. Personnel incidents include the capture, attempted recruitment, or control of personnel by a known or suspected hostile intelligence entity, or the unauthorized absence or defection of personnel having knowledge of or access to COMSEC information or material. Report these incidents by message (see Attachments 4 and 7).

2.3. Physical Incidents. Physical incidents include loss of control, lost material, theft, capture, recovery by salvage, tampering, unauthorized viewing and access, photographing, or copying that can potentially jeopardize COMSEC material. Report physical incidents by message (see Attachments 4 and 5). Examples include:

2.3.1. Unauthorized access to COMSEC material.

2.3.2. COMSEC material found outside required physical control. Examples include:

2.3.2.1. Finding COMSEC material documented as being destroyed.

2.3.2.2. COMSEC material left unsecured.

2.3.3. COMSEC material improperly packaged, shipped, or received with a damaged inner wrapper.

2.3.4. Destruction of COMSEC material by other than authorized means, not properly performed and documented (i.e., only one person destroying), or COMSEC material not completely destroyed and left unattended.

2.3.5. Actual or attempted unauthorized maintenance (including maintenance by unqualified personnel) or using a maintenance procedure that deviates from established standards.

2.3.6. Tampering with or penetration of a cryptosystem. Examples include:

2.3.6.1. Known or suspected tampering with, or unauthorized modification of, COMSEC material or its associated protective technology.

2.3.6.2. Finding an electronic surveillance or recording device in or near a COMSEC facility.

2.3.6.3. Activation of the antitamper mechanism on, or unexplained zeroization of, COMSEC equipment when other signs of unauthorized access or penetration are present. NOTE: Hold information concerning tampering with COMSEC equipment, penetration of protective technologies, or clandestine devices on a strict need-to-know basis. Immediately report by the most secure means to NSA, Air Force Office of Special Investigations (AFOSI) or Federal Bureau of Investigation, the controlling authority, and HQ AFCA/GCIS. When tampering or penetration is known or suspected, wrap and seal the material along with all protective technologies and place the package in the most secure, limited-access storage available. Do not use or otherwise disturb the material until further instructions are received from NSA. When a clandestine surveillance or recording device is suspected, do not discuss it in the area of the device, or anywhere else you suspect a device is installed. Take no action that will alert the clandestine activity, except on instruction from the applicable counterintelligence organization or NSA. Take no action that will jeopardize potential evidence.

2.3.7. Unexplained removal of keying material from its protective technology or unexplained loose keycards in an end-opening package.

2.3.8. Unauthorized reproduction or photographing of COMSEC material. (Manual cryptosystems can be locally reproduced as necessary to meet operational requirements per AFI 33-215, *Controlling Authorities for COMSEC Keying Material*.)

2.3.9. Deliberate falsification of COMSEC records.

2.3.10. Loss of two-person integrity or violation of COMSEC no-lone zone for Top Secret keying material (see AFKAG-1, *Air Force Communications Security [COMSEC] Operations*).

2.3.11. Incidents involving CCIs. Report those incidents where:

2.3.11.1. There is a determination that a CCI may be lost and cannot be accounted for. NOTE: Get information for the final report from the results of the report of survey or conduct an inquiry according to this AFI. In either case, format and report the information according to **Attachment 7**.

2.3.11.2. There is evidence of possible tampering with, or unauthorized access to or modification of, a CCI.

2.3.11.3. There are indications of known or suspected theft of a CCI.

2.3.11.4. A CCI is shipped in anything other than a zeroized or unkeyed condition and the shipping activity failed to get prior authorization according to AFKAG-1.

2.3.12. Report of suspected tampering or penetration of a "protected distribution system."

2.3.13. Aircraft crashes or disasters (natural, bomb, fire, etc.):

2.3.13.1. Use **Attachment 4** and **Attachment 5** to report aircraft and disaster incidents.

2.3.13.2. These incidents will be assigned "A" (aircraft) and "D" (disaster) plus the Air Force-assigned case number and MAJCOM. Aircraft and disaster incidents are only assigned case numbers and tracked under the purview of this AFI to clear the accounting records of any COMSEC material involved and to follow any recovery efforts, if practicable.

2.3.13.3. A formal inquiry is not required for aircraft and disaster incidents. For aircraft incidents, the report must identify where the aircraft crashed, progress of recovery efforts, circumstances involving recovery, what material was recovered and the extent of damage, what material was not recovered and the most likely disposition (e.g., destroyed in crash, retrieved by enemy, recovered by uncleared rescue personnel and turned over to security police, etc.). For disaster incidents, the report must identify progress of recovery efforts, circumstances involving recovery, the extent of damage to recovered material, what material was not recovered, etc.

2.3.14. Any other incident that jeopardizes the physical security of COMSEC material. (**NOTE:** Production errors and reports of defective keying material are not considered COMSEC incidents. These types of discrepancies are reported to NSA/V51A and Y265.)

3. Reporting Incidents:

3.1. Report incidents using this AFI in addition to the directives shown below:

3.1.1. Report incidents involving North Atlantic Treaty Organization (NATO) COMSEC material as prescribed in AMSG-293, *NATO Cryptographic Instructions*.

3.1.2. Report incidents involving communications-electronics operating instructions and status information of keying material according to AFI 31-401, *Managing the Information Security Program.*

3.1.3. Report PCM incidents according to CJCSI 3260.01.

3.1.4. Refer to Air Force COMSEC Publication (AFSAL) 4001A, *Controlled Cryptographic Items*, (will convert to AFSSI 4001, *Controlled Cryptographic Items*) for additional instructions regarding COMSEC equipment designated CCI.

3.2. National COMSEC Incident Reporting System. To remain effective, the National COMSEC Incident Reporting System must receive prompt and clear information about the incident. This information is critical to provide damage assessment by the evaluating authority. NSA continually evaluates the security of cryptosystems used by the United States Government. Each incident, regardless of how minor it may seem, when compared to other reports or information, often reveals weaknesses in procedures, systems, or personnel that can result in compromises. Therefore:

3.2.1. Every person possessing, handling, operating, maintaining, or repairing COMSEC material must stay thoroughly familiar with applicable physical and cryptographic security rules and will immediately report COMSEC incidents to the COMSEC responsible officer (CRO) or the commander. Failure to promptly report an incident may seriously affect the security of the cryptosystem involved and the defense of the United States. The CRO or commander reports the incident to the COMSEC manager. The COMSEC manager, using the information provided by the CRO or commander, reports the incident as prescribed in this publication (see **Attachment 3**).

3.2.2. Any person or activity detecting or suspecting that an incident involving COMSEC has occurred is responsible for reporting it in accordance with this instruction (see **Attachment 3**).

3.3. AFOSI Involvement in COMSEC Investigations. When the commander of the violating unit determines that the AFOSI should assume the investigation of a COMSEC incident, the violating unit stops its inquiry or investigation. During this period, the commander of the violating unit submits amplifying message reports every 30 days, indicating the AFOSI investigation is still ongoing (see **Attachment 6**). When AFOSI provides its final report, the commander reviews it with the COMSEC manager and sends it through COMSEC incident channels.

4. Roles and Responsibilities:

4.1. NSA/V51A:

4.1.1. Evaluates all cryptographic, personnel, aircraft, disaster COMSEC incidents and incidents involving COMSEC equipment.

4.1.2. Evaluates all physical COMSEC incident reports involving keying material in transit or if the controlling authority cannot be identified.

4.1.3. Evaluates all physical COMSEC incidents involving multiple controlling authorities of more than one department or agency.

4.1.4. Evaluates all reported COMSEC incidents concerning tampering, sabotage, evidence of covert penetration of packages, evidence of unauthorized or unexplained modification of COMSEC equipment, security containers, or vaults where COMSEC material is stored, and COMSEC material other than keying material (e.g., documents, algorithms, logic).

4.1.5. Evaluates, or coordinates evaluation of, COMSEC incidents having significant cryptologistic impact, and direct supersession of compromised future keying material that has not reached the COMSEC account.

4.1.6. Initiates or recommends appropriate action when COMSEC material is subjected to compromise, and notifies appropriate authorities of actions taken.

4.2. HQ AFCA/GCIS:

4.2.1. Manages the Air Force COMSEC Incident Program and serves as the Air Force COMSEC incident monitoring activity.

4.2.2. Assigns Air Force COMSEC incident case numbers. Case numbers are comprised of the violating unit's MAJCOM acronym followed by a “P” (for physical), “C” (for cryptographic), “H” (for personnel), “A” (for aircraft), or a “D” (for disaster), followed by the next unused case number for that MAJCOM, and the year the incident took place.

4.2.3. Evaluates physical COMSEC incidents involving multiple Air Force controlling authorities.

4.2.4. Evaluates COMSEC incidents involving a single Air Force controlling authority when the Air Force controlling authority causes the incident.

4.2.5. Exercises adjudication authority on whether a reported COMSEC incident has resulted in a COMSEC insecurity. Closes incident reports and upgrades incidents to insecurities, if appropriate.

4.2.6. Provides case status information to all appropriate addressees: case assignment within five working days upon receipt of report; case closure within 10 working days upon receipt of all required actions, to include the evaluation rendered by the controlling authority.

4.2.7. Maintains data base files to support the COMSEC Incident Trend Analysis (CITA) data base in collaboration with NSA.

4.2.8. Furnishes NSA information about the CITA data base for trends analysis and damage assessment associated with COMSEC incidents.

4.3. MAJCOMs:

4.3.1. Ensure all required reports are submitted and the controlling authority evaluation is completed before recommending case closure involving units under their purview.

4.3.2. Assess and provide comments on the appropriateness and effectiveness of actions planned or implemented to prevent COMSEC incidents from recurring.

4.3.3. Make sure COMSEC incident reports suspense dates are met.

4.3.4. Uses trend analysis as a management tool, showing the possibility of needed additional training or adjustment of personnel duty assignments.

4.4. Controlling Authorities:

4.4.1. Evaluate the security impact involving material they control, when physical incidents affect superseded, current, and future cryptonet keying material held by the COMSEC account and users, except as stated in paragraphs 4.1 and 4.2.

4.4.2. Inform all required COMSEC addressees of evaluation results and may recommend changing the incident to an insecurity as soon as possible, but within time limits and terms listed in Attachment 9.

4.4.3. Direct emergency supersession of keying material held by the cryptonet members and immediately notify the appropriate agencies according to AFI 33-215. Each agency notified is responsible for notifying individual holders to whom distribution was made. This includes those in other departments, agencies, services or commands, or nations. When a system is declared compromised, do not use for further encryption unless it is operationally essential to send encrypted messages before the supersession date and another suitable cryptosystem is not available.

4.4.4. Direct emergency extensions of keying material cryptoperiods, when necessary according to AFI 33-215. **NOTE:** The organization that directed the electronic key generation performs the controlling authority functions unless those functions are delegated to another organization.

4.5. The COMSEC Manager:

4.5.1. Briefs the commander of the violating unit on options available regarding inquiry and or investigation.

4.5.2. Provides assistance to inquiry or investigative official.

4.5.3. Reviews and provides additional comments, including concurrence or nonconcurrence with the final report.

4.5.4. Upon receipt of information from the inquiry official/violating unit, prepares and forwards all required reports according to this AFI. **NOTE:** Ensure reports are addressed correctly and include all case numbers assigned, beginning with HQ AFCA/GCIS assigned number.

4.6. Violating Unit's Commander:

4.6.1. When notified that an incident has occurred, sends a draft initial COMSEC incident report to the supporting COMSEC manager.

4.6.2. Appoints an appropriately cleared and disinterested civilian (General Schedule-9 or above), senior noncommissioned officer (master sergeant, senior master sergeant, or chief master sergeant) or commissioned officer to conduct the inquiry or investigation (see **Attachment 8**).

4.6.3. Upgrades an inquiry to an investigation, if the seriousness of the incident warrants it.

4.6.4. Provides the status of the inquiry or investigation to the supporting COMSEC manager.

4.6.5. Provides comments and concurrence or nonconcurrence in final reports, and the conclusions of the AFOSI investigation of the COMSEC incident if the AFOSI was involved.

4.6.6. Corrects unit deficiencies that contribute to COMSEC incidents and insecurities.

4.7. The Inquiry or Investigating Official:

4.7.1. Conducts an inquiry or investigation using the information and procedural guidance outlined in AFI 31-401. This AFI, however, is used as the authority to conduct the inquiry or investigation.

4.7.2. Completes the inquiry or investigation without intervening temporary duty, leave, or other duties.

4.7.3. Advises the violating unit's commander and COMSEC manager of the status of the inquiry or investigation.

4.7.4. Provides amplifying reports according to paragraph 5.1.

4.7.5. Documents the results, makes recommendations to prevent recurrence, and forwards the final report to the violating unit's commander who reviews, endorses, and forwards it to the COMSEC managers, who forwards it through COMSEC channels.

4.8. CROs and Users:

4.8.1. Know the types of incidents that could result from improper handling, control, and destruction of COMSEC material.

4.8.2. Know the types of reportable equipment malfunctions or operator errors.

4.8.3. Report any known or suspected incidents to the violating unit's commander, COMSEC manager, CRO or alternate immediately. NOTE: Check paragraphs 2 and 6, and **Attachment 9** for more information on types of incidents and PDSs.

5. Reporting Procedures:

5.1. Reporting Procedures During Normal Operations:

5.1.1. When submitting initial and amplifying COMSEC incident reports during normal operations, assign the appropriate precedence and submit the report according to **Table 1.** Assign higher precedence to reports that have significant potential impact on security.

Table 1. Assigning Precedence to and Time Requirements for Submitting Initial/Amplifying COMSEC Incident Reports.

RULE	If the Incident Involves:	Assign the Action Addressees a Precedence of:	Assign the Information Addressees a Precedence of:	To the Initial and Amplifying Reports and Submit as Soon as Possible, but no Later Than:
1	Currently effective keying material.	Immediate	Immediate	24 hours after discovery of the incident or receipt of amplifying information
2	Defection, espionage, hostile cognizant agent activity, clandestine exploitation, tampering, sabotage, or unauthorized copying, reproduction, or photographing.	Immediate	Immediate	24 hours after discovery of the incident or receipt of amplifying information
3	Future keying material scheduled to become effective within 15 days.	Immediate	Priority	48 hours after discovery of the incident or receipt of amplifying information.
4	Future keying material scheduled to become effective in more than 15 days.	Priority	Routine	48 hours after discovery of the incident or receipt of amplifying information.
5	Superseded, reserve, or contingency keying material.	Priority	Routine	48 hours after discovery of the incident or receipt of amplifying information.
6	Material or information not identified above	Routine	Routine	72 hours after discovery of the incident or receipt of amplifying information.

5.1.2. Format reports according to the requirements in **Attachment 2**. Initial reports must include each of the paragraphs as shown in the attachment. If the reporting requirements of the paragraph shown in the attachment do not apply, state "not applicable." Submit reports only by message. Submit letter reports only if message capability is not available or if specifically requested.

5.1.3. Classify incident reports according to content. Mark unclassified reports "For Official Use Only." For guidance consult AFMAN 33-272 (S) *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information* (U); Department of Defense (DoD) 5200.1-R, *Information Security Program*, and AFI 31-401.

5.1.4. Do an initial report for each COMSEC incident. Do not delay reporting in administrative channels to gather more information. An amplifying report is submitted when new information is discovered or is requested by the evaluating authority. The initial or amplifying report may serve as the final report if it contains all information required by paragraph 5.1.5 (**NOTE:** If report is used as final report, it must state "Request this report be accepted as final report."), has sufficient information for the controlling authorities to evaluate the incident, and is accepted as a final report by HQ AFCA/GCIS. Initial and amplifying reports are authorized for transmission during MINI-

MIZE. **NOTE:** If a final report is not completed within 30 days of the initial report, you must submit an amplifying report through COMSEC channels every 30 days, with information on the status of the final report, until the final report is completed.

5.1.5. A final report is required for each COMSEC incident unless the initial or an amplifying report was accepted as the final report. The final report must include a word-for-word report of the results of all inquiries and investigations and must identify corrective measures taken or planned to lessen the possibility or recurrence. Additional actions required for the final report:

5.1.5.1. Do not send final reports during MINIMIZE. Assign ROUTINE precedence to final reports.

5.1.5.2. Send the report through the violating unit commander and supporting COMSEC manager for their additional comments and concurrence or nonconcurrence. The COMSEC manager then routes the report to all required addressees.

5.1.5.3. On receipt of the report of inquiry or investigation, the controlling authority (if not previously determined from the initial or amplifying COMSEC incident report) determines if (a) the incident is a compromise, (b) a compromise cannot be ruled out, or (c) no compromise, and may recommend upgrading the incident to an insecurity, if appropriate.

5.1.5.4. The MAJCOM provides comments and concurrence or nonconcurrence in message format to HQ AFCA/GCIS and all other required addressees within five workdays.

5.1.5.5. HQ AFCA/GCIS closes the case on receipt of all required correspondence within 10 workdays.

5.2. Reporting During Tactical Deployments:

5.2.1. During time-sensitive tactical deployments, detailed reporting requirements may not be possible. If so, submit abbreviated reports for physical incidents involving keying material where espionage is not suspected. The report answers the "who, what, where, when, and how" questions, and provides enough detail to enable the evaluating authority to determine if a compromise has occurred.

5.2.2. Immediately report loss of keying material during actual hostile actions to each controlling authority by the fastest means available to allow supersession or recovery actions. Use any available resource.

5.2.3. In many cases, immediate reporting to activities other than the controlling authority will serve no purpose. Individual incident reports are not needed when keying material scheduled for supersession within 48 hours is lost during actual hostilities and espionage is not suspected. Submit a periodic summary of all previously unreported incidents at the earliest opportunity (see **Table 2.**). The summary lists all material lost, dates, places, and brief circumstances of loss.

Table 2. Addressing COMSEC Incident Reports.

RULE	If the Incident is:	Send Action Message to:	Send Information Copy to:	The Incident is Evaluated by:
1	A physical incident involving only one controlling authority	Controlling Authority	HQ AFCA/GCIS NSA/V51A Violating Unit Violating Unit's MAJCOM Reporting Account's MAJCOM	Controlling Authority
2	A physical incident involving multiple Air Force controlling authorities	HQ AFCA/GCIS	Controlling Authorities NSA/V51A Violating Unit Violating Unit's MAJCOM Reporting Account's MAJCOM	HQ AFCA/GCIS
3	A physical incident involving a protected distribution system	HQ AFCA/GCIS	Violating Unit Violating Unit's MAJCOM Reporting Account's MAJCOM	HQ AFCA/SYS
4	A physical incident involving controlling authorities from more than one department or agency	NSA/V51A	Controlling Authorities HQ AFCA/GCIS Violating Unit Violating Unit's MAJCOM Reporting Account's MAJCOM	NSA/V51A
5	A physical incident and the controlling authority cannot be determined	NSA/V51A	HQ AFCA/GCIS Violating Unit Violating Unit's MAJCOM	NSA/V51A
6	A cryptographic incident or involves COMSEC equipment	NSA/V51A	Reporting Account's MAJCOM	NSA/V51A
7	A personnel incident	NSA/V51A	Controlling Authorities for each item they had access to HQ AFCA/GCIS Violating Unit Violating Unit's MAJCOM Reporting Account's MAJCOM	NSA/V51A

5.3. Evaluating Reports. Use the guidelines in **Attachment 9** to evaluate COMSEC incidents.

5.4. Disposal of Material Involved in a COMSEC Incident:

5.4.1. When material on hand is subjected to a physical or cryptographic incident, keep the material until receipt of HQ AFCA/GCIS case closure message as stated in paragraph 5.5, or prior disposition instructions are received.

5.4.2. When an incident involves use of superseded key, the violating unit must have the means to provide the controlling authority copies of all traffic transmitted if a traffic review is directed per AFI 33-215.

5.5. Removing Material Involved in a Physical Loss from COMSEC Accounting Records. HQ AFCA/GCIS issues a case closure message when the inquiry or investigation is completed and all information required in this AFI is received. Use the case closure message as the authority for destruction and dropping accountability for the material from account records. If the material involved appears on the next semiannual inventory, line through the applicable items and cite the case number and case closure date-time group (DTG) message, and state the case is closed in the remarks section to make sure the Air Force Central Office of Records can take appropriate action.

5.6. COMSEC Incident and Insecurity Trends:

5.6.1. HQ AFCA/GCIS will develop and send a COMSEC incident and insecurity trends summary to all MAJCOMs and the Air Force Communications and Information Center (AFCIC/SYNI) semiannually (no later than 31 January for July through December, and 31 July for January through June).

5.6.2. The summary will include the different types of physical and cryptographic incidents or insecurities, and the total number and the major cause of incidents and insecurities. Personnel, aircraft, and disaster incidents are not included in the summary.

5.6.3. MAJCOMs are encouraged to comment on the summaries and disseminate to their subordinate units.

6. Practices Dangerous to Security (PDS). A PDS has the potential to jeopardize the security of COMSEC material if allowed to recur. See **Table 3.** for reporting a PDS. An inquiry report is not required unless requested by the controlling authority, MAJCOM, or COMSEC manager.

Table 3. Reporting a Practices Dangerous to Security (PDS).

RULE	If the PDS Involves:	The COMSEC Manager:
1	Premature or out of sequence use of keying material without the approval of the controlling authority, as long as the material was not reused.	Sends a routine message action to the controlling authority, and information copy to the account's MAJCOM and the violating unit's MAJCOM, within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
2	Inadvertent destruction of keying material. Destruction without authorization of the controlling authority, as long as the destruction was properly performed and documented.	Sends a routine message action to the controlling authority, and information copy to the account's MAJCOM and the violating unit's MAJCOM, within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
3	Removing keying material from its protective technology before issue for use. Removing the protective technology without authorization, so long as the removal was documented and there is no evidence of espionage.	Sends a routine message action to the controlling authority, and information copy to the account's MAJCOM and the violating unit's MAJCOM, within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
4	Unclassified accounting legend code (ALC)-1 material.	Sends a routine message action to the controlling authority, and information copy to the account's MAJCOM and the violating unit's MAJCOM, within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.

RULE	If the PDS Involves:	The COMSEC Manager:
5	Classified ALC-4 material.	Sends a routine message action to the controlling authority, and information copy to the account's MAJCOM and the violating unit's MAJCOM, within 3 duty days of notification, or sooner if specified by controlling authority instructions or if circumstances warrant. Complete any actions requested by the controlling authority or MAJCOMs.
6	Receiving a package with a damaged outer wrapper in which the inner wrapper is intact,	Does not report the PDS upchannel. Resolves the situation locally.
7	Unclassified ALC-4 material.	Does not report the PDS upchannel. Resolves the situation locally.
8	Activating the antitamper mechanism on or unexplained zeroization of COMSEC equipment when no other signs of unauthorized access or penetration are present.	Does not report the PDS upchannel. Resolves the situation locally.
9	Failure to zeroize a common fill device when a time limit is imposed.	Does not report the PDS upchannel. Resolves the situation locally.
10	Destruction of COMSEC material not performed within required time limits, as long as the material was properly stored or safeguarded.	Does not report the PDS upchannel. Resolves the situation locally.

WILLIAM J. DONAHUE, Lieutenant General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

References

AFI 33-215, *Controlling Authorities for COMSEC Keying Material*

AFI 31-401, *Managing the Information Security Program*

AFI 37-124, *The Information Collections and Reports Management Program; Controlling Internal, Public, and InterAgency Air Force Information Collections*

AFMAN 33-270, *Command, Control, Communications, and Computer (C4) Systems Security Glossary* (to be renamed *Information Protection Glossary* when current draft is published)

AFMAN 33-272, (S) *Classifying Communications Security, TEMPEST, and C4 Systems Security Research and Development Information* (U)

AFKAG-1, *Air Force Communications Security (COMSEC) Operations*

AFSAL 4001A, *Controlled Cryptographic Items* (will convert to AFSSI 4001, *Controlled Cryptographic Items*)

AMSG-293, *NATO Cryptographic Instructions*

CJCSI 3260.01, (S) *Joint Policy Governing Positive Control Material and Devices (U)*

DoD 5200.1-R, *Information Security Program*

NSTISSI 4003, *Reporting and Evaluating COMSEC Incidents*

Abbreviations and Acronyms

ACN—Accounting Control Number

AFCA—Air Force Communications Agency

AFCIC—Air Force Communications and Information Center

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

ALC—Accounting Legend Code

CCI—Controlled Cryptographic Item

CITA—COMSEC Incident Trend Analysis

CJCSI—Chairman of the Joint Chiefs of Staff Instruction

COMSEC—Communications Security

CRO—COMSEC Responsible Officer

Crypto—Cryptographic

DIRNSA—Director, National Security Agency

DoD—Department of Defense

DSN—Defense Switched Network

DTG—Date-Time Group

EKMS—Electronic Key Management System

JCS—Joint Chiefs of Staff

MAJCOM—Major Command

NATO—North Atlantic Treaty Organization

NCO—Noncommissioned Officer

NSTISSI—National Security Telecommunications and Information Systems Security Instruction

NSA—National Security Agency

PCM—Positive Control Material

PDS—Practices Dangerous to Security

POC—Point of Contact

Terms

Access—A condition where an individual has the opportunity and ability to obtain knowledge of, use, copy, remove, or tamper with COMSEC material. A person does not have access merely by being in a place where COMSEC material is kept as long as security measures (i.e., physical controls or authorized escort) deny opportunity to observe the material.

Communications Security (COMSEC) Facility—Space employed primarily for generating, storing, repairing, or using COMSEC material.

Cryptosecurity—Component of COMSEC that results from the provisions of technically sound cryptosystems and their proper use**.**

Electronically Generated Key—Key produced in nonphysical form by the National Security Agency (NSA) or at locations designated or approved by NSA. Electronically generated keys may exist only in nonphysical form (in a computer memory or in COMSEC equipment) or stored on a physical medium such as a floppy disk. Electronically generated keys stored on a physical medium are never considered "hard copy." Electronically generated keys are divided into two groups: 1. Field-Generated Electronic Keys. Used primarily for tactical communications nets in an operational environment. Normally used only to provide security for perishable, time-sensitive communications. Mobile facilities in the field or fixed COMSEC facilities may produce field-generated electronic keys. 2. Electronic Key Management System (EKMS)-Generated Electronic Keys: Used primarily for planned, static applications with well-defined net membership. Used to provide security for non-perishable information requiring a high degree of security. EKMS-generated key is produced at fixed COMSEC facilities.

Plain Text—Unencrypted information.

Protective Technologies—Special tamper-evident features and material applied to keying material packages and cryptographic equipment used to detect and deter possible compromise of COMSEC products such as tape canisters, end-opening keycard packages, holographic bags, seals, screw-head coatings, and logo tapes. These technologies provide evidence of tampering with items, and deter attempts by adversaries to gain access to equipment and keying material.

MINIMIZE—A condition where normal message and telephone traffic is drastically reduced so that messages connected with an actual or simulated emergency are not delayed.

Physical Security—The part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft.

Positive Control Material (PCM)—Includes sealed authentication systems, permissive action links, and positive enable material.

Protective Distribution System—A wireline or fiber optics distribution system with adequate electrical, electromagnetic, and physical safeguards to permit its use for transmission of unencrypted classified information. **NOTE:** This definition does not include intrusion detection optical communications systems approved by the National Security Agency.

Protective Packaging—Packaging techniques for COMSEC material that discourage penetration, reveal that a penetration has occurred or was attempted, or inhibit viewing or copying of keying material before it is exposed for use.

Attachment 2

REQUIRED COMMUNICATIONS SECURITY (COMSEC) INCIDENT REPORT INFORMATION

A2.1. Subject. Consists of only the words "COMSEC Incident" followed by complete case number IF ALREADY ASSIGNED.

A2.2. References. Identify the reporting requirement and all previous related messages and correspondence.

A2.3. Point of Contact (POC). Include name, COMSEC account number, secure telephone number, Defense Switched Network (DSN) telephone number, and commercial telephone number of an individual who is prepared to respond to questions concerning the incident.

A2.4. Communications Security Account. COMSEC account number supporting the unit responsible for the incident.

A2.4.1. Includes the violating unit and its major command (MAJCOM).

A2.5. Material Involved:

A2.5.1. For Hard-Copy Keying Material, Hard-Copy Key-in Electronic Form, and Documents. List the short title, edition, register number, specific segments, accounting legend code (ALC), classification of material, tables, pages, etc., if not a complete edition or document; and date stamped on the protective technology, if applicable. The controlling authority for each short title **MUST BE** stated by each piece of material on the initial COMSEC incident message report.

A2.5.2. For Electronically Generated Key. List the key designator, tag, or other identifier; circuit designator; type of crypto equipment used to secure the circuit; type of key generator ALC; and classification of material.

A2.5.3. For Equipment. List the system designator or nomenclature; modification number, if applicable; serial number of ALC-1 material (all other by quantity); serial number on the protective technology, if applicable; and associated or host equipment. If the equipment was keyed, provide the information required for keying material.

A2.6. Personnel Involved in the Incident. For each individual, provide name and grade, citizenship, duty position, military or civilian occupation specialty, level of security clearance, and parent MAJCOM.

A2.7. Circumstances of the Incident. Give a clear chronological account of the events that caused the incident. The chronology includes all dates, times, frequency of events, precise locations and organizational elements, etc.. If the reason for the incident is not known, describe the events that led to the discovery of the incident. Include a description of the security measures in effect at the location and estimate the possibility of unauthorized personnel gaining access to the material.

A2.8. Possibility of Compromise. Provide an opinion as to the possibility of compromise and the basis for the opinion.

A2.9. Additional Reporting Requirements When Incident Involves:

A2.9.1. Incorrect Use of COMSEC Keying:

A2.9.1.1. Describe the communications activity (e.g., COMSEC keying on-line/off-line, simplex/half-duplex/full-duplex, point-to-point/netted operations).

A2.9.1.2. Describe the operating mode of the crypto equipment (e.g., clock start, message indicator).

A2.9.2. Use of Unapproved Operating Procedures:

A2.9.2.1. Estimate the amount and type of traffic involved.

A2.9.2.2. Estimate the length of time the key was used.

A2.9.3. Use of Malfunctioning COMSEC Equipment:

A2.9.3.1. Describe the symptoms of the malfunction.

A2.9.3.2. Estimate the likelihood that the malfunction was deliberately induced. If so, also refer to paragraph A2.9.5.

A2.9.3.3. Estimate how long the malfunctioning equipment was in use.

A2.9.3.4. Estimate the amount and type of traffic involved.

A2.9.4. Unauthorized Modification or Discovery of a Clandestine Electronic Surveillance or Recording Device in or Near a COMSEC Facility:

A2.9.4.1. Describe the modification or monitoring device, installation, symptoms, host maintenance of COMSEC equipment involved, and protective equipment technology, if applicable.

A2.9.4.2. Estimate how long the item was in place.

A2.9.4.3. Estimate the amount and type of traffic involved.

A2.9.4.4. Identify the counterintelligence organization (e.g., AFOSI), a POC, and telephone number.

A2.9.5. Known or Suspected Defection, Hostile Cognizant Agent Activity, Attempted Recruitment, Espionage, Sabotage, Treason, Capture, or Unauthorized Absence:

A2.9.5.1. Describe the individual's general background in COMSEC and the extent of knowledge of crypto principles and protective technologies.

A2.9.5.2. List the cryptosystems that the individual had access to and whether the access was to cryptographic logic or keying material. For logic, state whether access was too full or limited maintenance manuals; for keying material, list the short titles and editions involved.

A2.9.5.3. Identify the counterintelligence organization (e.g., AFOSI), a POC, and telephone number.

A2.9.6. Unauthorized Access to COMSEC Material:

A2.9.6.1. Estimate how long unauthorized personnel had access to the material.

A2.9.6.2. State whether espionage is suspected. If espionage is suspected, refer to paragraph A2.9.5.

A2.9.7. Loss of COMSEC Material:

A2.9.7.1. Describe the circumstances of last sighting. Provide all available information concerning the cause of disappearance.

A2.9.7.2. Describe actions taken to locate the material. **Note:** Consider the possibility that material was removed by authorized or unauthorized persons.

A2.9.7.3. Describe the methods of disposal of classified and unclassified waste and the possibility of loss by those methods.

A2.9.8. COMSEC Material Discovered Outside of Required COMSEC Accountability or Control:

A2.9.8.1. Describe the action that restored accountability or physical control.

A2.9.8.2. Estimate the likelihood of unauthorized access.

A2.9.8.3. Estimate the time the material was unsecured.

A2.9.9. COMSEC Material Received with a Damaged Inner Wrapper:

A2.9.9.1. Give a complete description of the damage.

A2.9.9.2. Describe situations where damage occurred in transit and identify the mode of transportation. Include the package number and point of origin.

A2.9.9.3. Describe how the material was stored if the damage occurred in storage.

A2.9.9.4. Estimate the likelihood of unauthorized access or viewing.

A2.9.9.5. Retain all packaging containers, wrappers, etc., until destruction is authorized.

A2.9.10. Known or Evidence of Suspected Tampering with COMSEC Material:

A2.9.10.1. Describe the evidence of tampering.

A2.9.10.2. Identify the mode of transportation if the suspected tampering occurred in transportation. Include the package number and point of origin.

A2.9.10.3. Describe how the material was stored if the suspected tampering occurred in storage.

A2.9.10.4. Identify the counterintelligence organization (e.g., AFOSI), a POC, and telephone number.

A2.9.10.5. Identify the date stamped on the protective technology, or serial number on the protective technology, if applicable.

A2.9.11. Unauthorized Reproduction or Photography:

A2.9.11.1. Identify the material or equipment reproduced or photographed.

A2.9.11.2. Provide the reason for the reproduction and describe how the material was controlled.

A2.9.11.3. Specify how detailed the photographs of equipment internals were.

A2.9.11.4. State whether espionage is suspected. If espionage is suspected, refer to paragraph A2.9.5.

A2.9.11.5. Forward copies of each photograph or reproduction to Director, National Security Agency (DIRNSA/V51A) and HQ AFCA/GCIS.

A2.9.12. Aircraft Crash/Disaster Incidents:

A2.9.12.1. Identify the location and coordinates of the crash/site of disaster, and specify whether the crash/disaster incident was in friendly or hostile territory. If an aircraft incident is at sea, refer to paragraph A2.9.13.

A2.9.12.2. State whether the aircraft/material involved in disaster remained largely intact or if wreckage/material was scattered over a large area. Estimate the size of the area.

A2.9.12.3. State whether the area was secured. If the area was secured, state how soon after the crash/disaster incident and by whom.

A2.9.12.4. State whether recovery efforts for COMSEC material were made or are anticipated, and the circumstances involving recovery.

A2.9.12.4.1. State what material was recovered and the extent of damage.

A2.9.12.4.2. State what material was not recovered and the most likely disposition (e.g., destroyed in crash/disaster, retrieved by enemy, recovered by uncleared rescue personnel and turned over to security police, etc.).

A2.9.13. Material Lost at Sea:

A2.9.13.1. Provide the coordinates (when available) or the approximate distance and direction from shore.

A2.9.13.2. Estimate the depth of the water.

A2.9.13.3. State whether material was in weighted containers or was observed sinking.

A2.9.13.4. Estimate the sea state, tidal tendency, and the most probable landfall.

A2.9.13.5. State whether United States salvage efforts were made or are anticipated.

A2.9.13.6. State whether foreign vessels were in the immediate area and their registry, if known.

A2.9.13.7. Estimate the possibility of successful salvage operations by unfriendly nations.

A2.9.14. Space Vehicles:

A2.9.14.1. Provide the launch date and time.

A2.9.14.2. State whether the space vehicle was destroyed or lost in space.

A2.9.14.3. State whether the keying material involved was unique to the operation or is common to other operations.

A2.9.14.4. Estimate the probable impact point on the Earth's surface, if applicable. If the impact point was on land, refer to paragraph A2.9.12; if at sea, refer to paragraph A2.9.13.

Attachment 3

SAMPLE--INITIAL PHYSICAL COMMUNICATIONS SECURITY (COMSEC) INCIDENT REPORT

FM: UNIT/BASE/CAXXXXXX//

TO: *(See Figure 5.2)*

INFO: *(See Figure 5.2)*

SUPPORTING COMSEC ACCOUNT'S MAJCOM COMSEC DIRECTORATE//

VIOLATING UNIT'S MAJCOM COMSEC DIRECTORATE//

DIRNSA FT GEORGE G MEADE MD//V51A//*(UNLESS AN ACTION ADDRESSEE)*

C L A S S I F I C A T I O N (**NOTE:** *As a Minimum Mark "For Official Use Only"*)

MSGID/GENADMIN/*SENDER'S OFFICE*/-/*MONTH*//

SUBJ/COMSEC INCIDENT--INITIAL REPORT//

REF/A/AFI 33-212, PARA 2.3, AS APPLICABLE//

REF/B/*OTHER APPLICABLE DOCUMENTS*//

REF/C/*ADDITIONAL RELATED CORRESPONDENCE AND MESSAGES ON INCIDENT*//

POC/*NAME*/*TITLE*/*UNIT*/*LOC:*/*TEL: DSN*//

RMKS/1. COMSEC ACCOUNT: *XXXXXX*.

A. VIOLATING UNIT:

B. MAJCOM OF VIOLATING UNIT:

2. MATERIAL INVOLVED: *LIST ALL MATERIAL INVOLVED IN INCIDENT INCLUDING SHORT TITLE, EDITION, ACCOUNTING CONTROL NUMBER (ACN), CONTROLLING AUTHORITY, CLASSIFICATION, AND ACCOUNTING LEGEND CODE (ALC) FOR EACH ITEM INVOLVED.*

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: *COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE*.

6. ADDITIONAL REPORTING REQUIRED BY AFI 33-212 (*See* **Attachment 2**).

Attachment 4

SAMPLE--INITIAL CRYPTOGRAPHIC COMMUNICATIONS SECURITY (COMSEC) INCIDENT REPORT

FM: UNIT/BASE/CAXXXXXX//

TO: DIRNSA FT GEORGE G MEADE MD//V51A//

INFO: HQ AFCA SCOTT AFB IL//SYSC//

ACTUAL CONTROLLING AUTHORITIES//

SUPPORTING COMSEC ACCOUNT'S MAJCOM COMSEC DIRECTORATE

VIOLATING UNIT'S MAJCOM COMSEC DIRECTORATE

C L A S S I F I C A T I O N (**NOTE:** As a Minimum Mark "For Official Use Only")

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT--INITIAL REPORT//

REF/A/AFI 33-212, PARA 2.1//

REF/B/OTHER APPLICABLE DOCUMENTS//

REF/C/ADDITIONAL RELATED CORRESPONDENCE AND MESSAGES ON INCIDENT//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

A. VIOLATING UNIT:

B. MAJCOM OF VIOLATING UNIT:

2. MATERIAL INVOLVED: LIST ALL MATERIAL INVOLVED IN INCIDENT, INCLUDING SHORT TITLE, EDITION, ACCOUNTING CONTROL NUMBER (ACN), CONTROLLING AUTHORITY, CLASSIFICATION, AND ACCOUNTING LEGEND CODE (ALC) FOR EACH ITEM INVOLVED.

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING AS REQUIRED BY AFI 33-212 (*See* **Attachment 2**).

Attachment 5

SAMPLE--PERSONNEL COMMUNICATIONS SECURITY (COMSEC) INCIDENT REPORT

FM: UNIT/BASE/COMSEC ACCOUNT//

TO: DIRNSA FT GEORGE G MEADE MD//V51A//

INFO: HQ AFCA SCOTT AFB IL//SYSC//

SUPPORTING ACCOUNT'S MAJCOM COMSEC DIRECTORATE//

VIOLATING UNIT'S MAJCOM COMSEC DIRECTORATE//

CONTROLLING AUTHORITIES//

C L A S S I F I C A T I O N (**NOTE:** AS A MINIMUM MARK "FOR OFFICIAL USE ONLY")

MSGID/GENADMIN/SENDER'S OFFICE/-/MONTH//

SUBJ/COMSEC PERSONNEL INCIDENT//

REF/A/AFI 33-212, PARA 2.2

REF/B/ADDITIONAL RELATED CORRESPONDENCE AND MESSAGES ON INCIDENT.//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN//

RMKS/1. COMSEC ACCOUNT: XXXXXX.

2. MATERIAL INVOLVED: LIST ALL MATERIAL INVOLVED IN INCIDENT INCLUDING SHORT TITLE, EDITION, ACN CONTROLLING AUTHORITY, CLASSIFICATION, AND ALC FOR EACH ITEM INVOLVED.

3. PERSONNEL INVOLVED IN THE INCIDENT:

4. CIRCUMSTANCES OF INCIDENT:

5. INITIAL INCIDENT ASSESSMENT: COMPROMISE, COMPROMISE CANNOT BE RULED OUT, OR NO COMPROMISE.

6. ADDITIONAL REPORTING REQUIRED BY AFI 33-212 (*See* **Attachment 2**).

Attachment 6

SAMPLE--AMPLIFYING COMMUNICATIONS SECURITY (COMSEC) INCIDENT REPORT

FM: UNIT/BASE/COMSEC ACCOUNT//

TO: SAME AS INITIAL REPORT

INFO: ALL INFO ADDRESSEES (SAME AS ON INITIAL REPORT)//

C L A S S I F I C A T I O N (**NOTE:** AS A MINIMUM MARK “FOR OFFICIAL USE ONLY”)

MSGID/GENADMIN/SENDERS OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT (AIR FORCE COMPLETE ASSIGNED CASE NUMBER AND ALL OTHER AGENCIES ASSIGNED CASE NUMBERS) AMPLIFYING REPORT//

REF/A/REFERENCE THE DATE-TIME GROUP (DTG) OF INITIAL REPORT AND UNIT IDENTIFIER//

REF/B/ADDITIONAL MESSAGE/CORRESPONDENCE RELATING TO THE INCIDENT//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN//

RMKS/1. AMPLIFYING REPORTS SHOULD PROVIDE ANY NEW INFORMATION, OR ANY INFORMATION THAT WAS OMITTED FROM THE INITIAL REPORT, WHICH CAN HELP EVALUATE THE INCIDENT.

WHERE INFORMATION HAS NOT CHANGED, EACH ITEM IS ANNOTATED WITH "N/A." INCLUDE ANY NEW INFORMATION.

THIS REPORT CAN BE USED FOR STATUS OF THE ONGOING REPORT IF NOT COMPLETED IN THE REQUIRED TIME LIMIT.//

Attachment 7

SAMPLE--FINAL COMMUNICATIONS SECURITY (COMSEC) INCIDENT REPORT

FM: UNIT/BASE/COMSEC ACCOUNT//

TO: SAME AS INITIAL REPORT//

INFO: SAME AS INITIAL REPORT//

C L A S S I F I C A T I O N (**NOTE:** AS A MINIMUM MARK "FOR OFFICIAL USE ONLY")

MSGID/GENADMIN//SENDERS OFFICE/-/MONTH//

SUBJ/COMSEC INCIDENT (COMPLETE CASE NUMBER AND ALL OTHER AGENCIES ASSIGNED CASE NUMBERS)--FINAL REPORT//

REF/A/REFERENCE THE DATE-TIME GROUP (DTG) AND UNIT IDENTIFIER OF INITIAL REPORT//

REF/B/REFERENCE ALL OTHER MESSAGE/CORRESPONDENCE RELATING TO THE INCIDENT//

POC/NAME/TITLE/UNIT/LOC:/TEL: DSN//

RMKS/1. PART 1: THE INQUIRY OFFICER'S REPORT VERBATIM.

2. PART 2: MUST INCLUDE THE VIOLATING UNIT COMMANDER'S COMMENTS.

3. PART 3: MUST INCLUDE THE COMSEC MANAGER'S COMMENTS.//

Attachment 8

SAMPLE--APPOINTMENT MEMORANDUM OF INQUIRY (OR INVESTIGATING) OFFICIAL

MEMORANDUM FOR MAJOR JOHN JONES

FROM: 932 AAW/CC

203 W. Losey Street, Room 1234

Scott AFB IL 62225-1234

SUBJECT: Appointment of COMSEC Inquiry (or Investigating) Official

1. You are appointed to perform the duties of an inquiry (or investigating) official as outlined in AFI 33-212, *Reporting COMSEC Incidents*. As the appointed official, you are my personal representative in this matter. Your primary duties are to conduct an inquiry (or investigation) into the *(state reason for appointment)*, to determine if a compromise has occurred, and to prepare a report according to AFI 31-401, *Managing the Information Security Program*, and appropriate attachments. Second, you are to determine if COMSEC weaknesses exist that need to be addressed.

2. You are to gather the facts surrounding the incident and to make recommendations based on those facts. You **DO NOT** evaluate COMSEC incidents; that decision is made by the controlling authority.

3. Process your report through me. The report is due by *(15 days from the date of the initial report)*. If you cannot meet the deadline, contact my office immediately.

4. Point of contact throughout this inquiry is *(name of POC)* at extension *XXXX*.

JOHN DOE, Colonel, USAF

Commander

Attachment 9

COMMUNICATIONS SECURITY (COMSEC) INCIDENT EVALUATION GUIDE

A9.1. Guidelines for Evaluating Communications Security Incidents.

A9.1.1. COMSEC incident evaluation and compromise recovery are two separate, distinct actions. Take compromise recovery actions as soon as possible according to AFI 33-215, Controlling Authorities for COMSEC Keying Material. Evaluation is an administrative adjudication that must be accomplished according to the time limits listed in A9.2, but must not be excessively influenced by any recovery actions that have already been taken. For example, if a controlling authority initiated precautionary supersession based on an initial report, and subsequent reports presented mitigating circumstances, the evaluating authority is not required to evaluate the incident as a compromise. Conversely, a controlling authority is not required to initiate precautionary supersession when an incident is evaluated as "compromise" or "compromise cannot be ruled out," if in the evaluating authority's opinion, supersession is not warranted or is not feasible.

A9.1.2. When evaluating incidents, consider the information stated in the report, the cryptosystem security characteristics, and the effect on the cryptosystem involved. Evaluate COMSEC incidents by using one of the following terms:

A9.1.2.1. Compromise. The material was irretrievably lost or available information clearly proves that the material was made available to an unauthorized person.

A9.1.2.2. Compromise Cannot Be Ruled Out. Available information indicates that the material could have been made available to an unauthorized person, but there was no clear proof that it was made available.

A9.1.2.3. No Compromise. Available information clearly proves that the material was not made available to an unauthorized individual.

A9.1.3. COMSEC incident evaluation is often a subjective process, even when the controlling authority has all pertinent facts. While it is not possible to discuss in this publication all possible types of COMSEC incidents that controlling authorities need to assess, the following guidelines are provided for consistency in assessing commonly encountered types. Complete guidelines for evaluating incidents involving Joint Chiefs of Staff (JCS) positive control material (PCM) are contained in CJCSI 3260.01, (S) Joint Policy Governing Positive Control Material and Devices (U).

A9.1.3.1. Lost keying material, including keying material believed destroyed without documentation, and material temporarily out of control (i.e., was believed lost but later recovered under circumstances where continuous secure handling was not assured or was found in an unauthorized location) should be evaluated as "compromise."

A9.1.3.2. Unauthorized access to keying material should be evaluated as "compromise." Access exists when an individual has the capability and opportunity to gain detailed knowledge of, or to alter information or material. An individual does not have access if that individual is under escort or under the observation of a person authorized access, or if physical controls prevent detailed knowledge or altering of information or material.

A9.1.3.3. Unauthorized absences of personnel with access to keying material are evaluated as "compromise cannot be ruled out" unless there is evidence of theft, loss of keying material, or defection. However, when an individual with prior access to keying material is officially reported by the commander as an unauthorized absentee, an immediate inventory is made of all material that individual had access to. If there is evidence of theft or loss of keying material, or defection of personnel, the controlling authority considers the material compromised and initiates emergency supersession.

A9.2. Time Limits for Evaluating Communications Security Incidents.

A9.2.1. Evaluate COMSEC incident reports within the time limits specified below. Time limits begin upon receipt of the initial or amplifying report if the initial report does not contain sufficient information to make an evaluation. The evaluating authority must solicit any information required to make an evaluation.

A9.2.2. Evaluate initial reports of the following incidents or respond within 24 hours:

A9.2.2.1. Currently effective keying material or keying material scheduled to become effective within 15 days.

A9.2.2.2. Defection; espionage; hostile cognizant agent activity; clandestine exploitation, tampering, penetration, or sabotage; or unauthorized copying, reproduction, or photography.

A9.2.3. Evaluate initial reports of the following incidents or respond within 48 hours:

A9.2.3.1. Future keying material scheduled to become effective beyond the next 15 days.

A9.2.3.2. Superseded, reserve, or contingency keying material.

A9.2.4. Evaluate initial reports of COMSEC incidents not covered above or respond within 5 duty days.