Washington State Fusion Center

Standard Operating Procedures

September 2009

Table of Contents

INTRODUCTION

The Standard Operating Procedure (SOP) is intended to serve as a guide and framework within which employees can make decisions and provide a broad outline of procedures for managing and regulating key conduct of Washington State Fusion Center (WSFC) functions. It is not intended to cover every situation that may arise in the course of one's duties. These procedures will be further developed as technology solutions and resources within the Fusion Center are realized.

SITUATIONAL AWARENESS

The Situational Awareness and Watch Center (SAWC) is the hub of WSFC operations for maintaining and sharing situational awareness and performing the central functions of intake, knowledge management, and dissemination.

- Situational Awareness within the Fusion Center is maintained through multiple sources, including but not limited to: law enforcement, private security, emergency management, and open source material.
- The Situational Awareness component of the WSFC maintains awareness of international, national, and regional activities that affect Washington State, as well as:
    - Significant events and incidents,
    - Special Event planning and operations,
    - Warning of public safety and security threats,
    - Washington State DOT Road Advisories, and
    - Severe weather advisories/warnings.

COLLECTION

The overall management and oversight of collection plans and operations rests with the Intelligence & Analysis Section, in collaboration with the SAWC and Sections within the Fusion Center.

Collection involves identifying what information the WSFC needs to perform its mission and meet its objectives, discerning which sources to collect the information from based on reliability and credibility, and undertaking steps to acquire the applicable information in a manner consistent with the legal guidelines outlining such practices for Fusion Centers.

Intelligence collection must be restricted to the gathering of information about persons or organizations reasonably suspected of intent to commit a crime or engaging in criminal activity. In all cases, a suspected criminal predicate must exist before information is collected and maintained on a particular person or group.

In all cases, if it is determined that a particular person or group is not involved in terrorism or criminal activity, all information related to that group or person must be purged from electronic and physical records. The WSFC's Civil Liberties & Privacy Protection Policy provides the framework for the collection of non-intelligence information.

WSFC collection requirements should utilize all sources of information to provide the opportunity for more accurate, informed situational awareness. Information may be collected from the following sources, for example:

- Records management systems
- Law enforcement, corrections and other local, regional, state and federal data sources
- Law enforcement operations and investigations
- Open source
- Public and private sector CIKR partners

COLLECTION PROCESSES

Generally, collection requirements fall into two categories, short-term collection and long-term collection. Short-term collection normally involves a narrow range of information required to address a specific issue, while long-term collection typically involves gathering information for longer periods of time to form a base of knowledge about a person or group's criminal or terrorism related activities to facilitate law enforcement operations.

SHORT-TERM COLLECTION

Short-term collection will be accomplished by querying resources that are readily available to analysts and issuing Requests for Information (RFI) to selected agencies describing the information needed.

1) Prior to issuing an RFI, all internal and external data sources should be researched to ensure that the needed information is not already available.
    a) RFI's should be issued when research determines that the needed information is not readily available and that a request to an external agency or agencies is the only avenue for obtaining the information.
2) RFI's will, at a minimum, include the following:
    a) Brief description of the issue upon which the RFI is based
    b) The sensitivity of the issue of interest
    c) A description of information needed
    d) The latest time information is of value
    e) Point of Contact information

LONG-TERM COLLECTION

Long-term collection usually involves a broad set of information requirements based on reasonable suspicion of criminal activity needed for the development of detailed knowledge to support analysis and investigations.

1) Long-term collection requires the continuous development of a collection plan by the Intelligence & Analysis Section that includes the following elements:
    a) Statement of the intelligence goal or goals which the collection plan and requirements support

b) Identification of the information gaps and prioritization of the types of information needed

c) Determination of potential best methods and sources for getting the information needed

2) The collection plan must be reviewed and approved by a WSFC Supervisor prior to dissemination.

3) Issue the plan within the WSFC and to the agencies that may have the information or the ability to access and acquire the information needed.

4) As information is reported, provide feedback to collecting agencies along with follow-up requests.

5) When the collection plan has served its purpose, notify all involved or aware that it is no longer in effect.

INTAKE AND ASSIGNING (TASKING)

The Intake function within the WSFC Situational Awareness and Watch Center (SAWC) shall be staffed during normal business hours, Monday through Friday, 0730-1630 hours (Pacific Standard Time), excluding holidays. During non-business hours and holidays, WSFC Hotline callers hear a recording that directs them to call the Western States Information Network (WSIN) to make their report. Reports are logged by WSIN and notification is made to a WSFC Supervisor, via the WSP Call Center, for reports that are urgent in nature.

All incoming reporting and requests for WSFC products and services will be channeled through the Intake process. The process includes receiving, documenting, categorizing, routing, and storing data.

Intake mechanisms utilized to receive data include the WSFC Hotline, Email, Fax, US Mail, and direct reporting to WSFC staff.

When incidents or threats have the potential for fatalities, multiple casualties, economic consequences, mass evacuations, national security implications, or other priority 1 incidents as described below the Intake and Dissemination Officer shall make immediate notification to the Duty Supervisor who will make additional notifications and coordinate initial response efforts.

INTAKE AND DISSEMINATION OFFICER

Upon receipt of data, the Intake and Dissemination Officer will:

1) Make a summary entry into the Daily Intake Log.

a) Categorize the data as:

i) Suspicious Activity Report

ii) Information

(1) Open Source Information

(2) Government Record

iii) Intelligence[1]
   (1) Criminal Nexus Identified
   (2) Intelligence Report from Partner Agency
iv) Request for WSFC Product, such as:
   (1) Bulletin
   (2) Threat Assessment
   (3) Officer Safety Bulletin
v) Request for WSFC Service, such as:
   (1) Briefing
   (2) Tour
   (3) Assistance with investigation
   (4) Tabletop exercise
vi) Other

b) Assign a unique WSFC tracking number.
c) Assign priority level.
   i) Priority Level 1 – Immediate processing
   ii) Priority Level 2 – Process by date identified
   iii) Priority Level 3 – No action required
d) Catalog the type of data:
   i) International Terrorism
   ii) Domestic Terrorism
   iii) Gangs
   iv) Maritime
   v) CBRNE
   vi) Significant Crimes
   vii) Critical Infrastructure
   viii) Other
e) Ensure Intake log reflects the following information:
   i) Date and time of occurrence(s)
   ii) Date, time and method of report to WSFC
   iii) Identity of the reporting person or requestor and their contact information if possible

[1] Meets 28 CFR Part 23 criteria for Intelligence.

2) Conduct preliminary review of the data for validity and determine if the data received falls within WSFC guidelines.
   a) Check data coming in against *appropriate* sources, for example:
      i) Law Enforcement Information Exchange (LINX)
      ii) FBI Systems
      iii) WAFUSION Intake Log
      iv) Regional Information Sharing System Database (RISS)
      v) Homeland Security State and Local Intelligence Community (HS SLIC)
      vi) Law Enforcement Online (LEO)
      vii) Washington State Emergency Management Department
      viii) DHS Infrastructure Protection Protective Security Advisor (LENS, IRIS)
   b) Obtain any official documents associated with report
3) Provide initial reports, documents, and a summary of action taken to the Duty Supervisor for determination of disposition or referral.
4) Communicate receipt of data and unique tracking number back to reporting party as directed by the Duty Supervisor.
   a) If the information is deemed to be appropriate, provide unique tracking number back to reporting party.
   b) If the information does not meet identified reporting guidelines, provide feedback to reporting party.
   c) If the information is malicious in nature, no response necessary.
5) Monitor and maintain a status of assigned items (tasks) to completion.
   a) The intake and assignment/task record will be updated when assignment/task status changes are received from WSFC Sections.
   b) Intermediate correspondence and final outcomes of assigned/tasked items will be affixed to the original intake report and will be stored to form a complete record of the assignment/task.

SAWC DUTY SUPERVISOR

The SAWC Duty Supervisor will:

1) Review and approve all data received in the Intake process.
2) Direct feedback to reporting party as appropriate
3) Determine Follow-up Action
   a) Refer to local, state and/or federal agency for Follow-up
   b) Refer to WSFC Section(s) for Follow-up
   c) Information Only or No Action Required

4) Provide documentation to appropriate WSFC Section Supervisors as determined by areas of responsibility. Notify Intake and Dissemination Officer who has been assigned lead responsibility for the task so that the Daily Intake Log can be updated.
5) Assign a WSFC information protection designation:
   a) Open Source[2]
      i) Information that can be obtained legally by request, purchase, or observation.
   b) Controlled Unclassified Information[3] (CUI)
      i) Categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is:
         (1) Pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government
         (2) Under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination
      ii) Includes categories such as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), and Sensitive But Unclassified (SBU).
   c) Protected Critical Infrastructure Information (PCII)
      i) Only the PCII Program Office or a PCII Program Manager Designee may mark information as PCII and provide it with a submission identification number. Information that does not contain the requisite PCII markings and identification number is not PCII. The PCII marking remains until the PCII Program Office determines that the information no longer qualifies for PCII protection or the submitter requests that the protection be removed.
      ii) PCII Authorized Users must ensure products created from PCII include a PCII cover sheet and are marked with "Protected Critical Infrastructure Information" in the headers and footers to alert users to the information's status and protection requirements.
   d) Classified Information
      i) Classified information shall not be stored in Fusion Center systems. It will be stored in appropriate federal systems/databases.
6) Ensure Intake Log is updated with status.

[2] "Open Source for Fusion Center Practitioners" manual definition, page 1

[3] http://www.archives.gov/cui/

WSFC SECTION SUPERVISOR

The WSFC Section Supervisor(s) will:

1) Review, assign and/or refer reports or requests for products and services as appropriate.
2) Monitor progress and work with the SAWC Duty Supervisor if a deadline needs to be reevaluated.
3) Ensure Intake Log is updated with current status.

ANALYSIS AND PROCESSING

SUSPICIOUS ACTIVITY REPORTS (SAR)

Suspicious Activity Reports (SAR) and Field Interview, or Field Information, Reports (FIR) are examples of mechanisms utilized to report suspicious activity.

The National SAR Initiative (NSI) is the mechanism for sharing SAR nationally. A SAR in this environment is referred to as an Information Sharing Environment Suspicious Activity Report (ISE-SAR).

Nationally, 'Suspicious Activity' is defined as observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. It is important to stress that SAR reporting is a behavior-focused approach; race, ethnicity, national origin, or religious affiliation shall not be considered as factors that create suspicion.

If the SAR meets the national definition, then it will be shared via the NSI process.

INTAKE AND DISSEMINATION OFFICER

SAR information will be stored in a WSFC database if it is found to meet the reporting guidelines outlined above. The SAR will be processed by the Intake and Dissemination Officer, according to the procedures below:

1) Assign SAR Category, as described in the ISE-SAR Criteria Guidance.
    a) Eliciting Information
    b) Breach/Attempted Intrusion
    c) Misrepresentation
    d) Photography
    e) Observation
    f) Surveillance
    g) Theft/Loss/Diversion
    h) Sabotage/Tampering/Vandalism
    i) Testing of Security
    j) Cyber Attack
    k) Expressed or Implied Threat

l) Flyover
m) Materials Acquisition/Storage
n) Weapon's Discovery
o) Sector-Specific Incident
p) Recruiting
q) Other

SAWC (DUTY) SUPERVISOR

The SAWC (Duty) Supervisor notifies and coordinates intake items with Regional and Statewide Support Sections, the Critical Infrastructure Section, and Intelligence and Analysis Section for disposition and tasking.

SECTION SUPERVISOR

The Section Supervisor tasked with primary follow-up responsibility, as appropriate, shall ensure that:

1) The Lead Investigator is identified
2) Collaborate with other WSFC Sections
3) Follow-up is conducted with due diligence
4) Appropriate notifications are made to partners, for example:
   a) First Responder Agencies (Police, Fire, Emergency Management)
   b) Law Enforcement Support Agencies
   c) Federal Agencies
   d) CIKR Representatives
5) Timelines are met
6) Log is updated as the investigation progresses, through final disposition

INFORMATION

Information is defined as data that is relevant to the mission and function of the WSFC, but does not meet the definition of Intelligence, per 28 CFR Part 23.

Information will be evaluated to determine its relevancy to the WSFC and its partners. Generally, this information will come from a variety of sources: law enforcement records, public sources, and private partners.

1) Duty Supervisor will ensure that:

   a) Incoming reports and products are routed to managers, supervisors and WSFC personnel *according to their subject matter roles* for situational awareness.

b) Incoming information is appropriately logged and stored in a WSFC database.

2) Duty Supervisor notifies and coordinates intake items with Regional and Statewide Support Sections and the Critical Infrastructure Section for disposition and tasking. The Intelligence and Analysis Section will support the process as requested.

   a) Section Supervisor ensures that Intake and Dissemination Officer is updated with current status.

3) Section Supervisor tasked with primary follow-up responsibility shall ensure that, as appropriate:

   a) The Lead Investigator and/or Analyst is identified.

   b) Collaborate with other WSFC Sections.

   c) Follow-up is conducted with due diligence.

   d) Appropriate notifications are made to partners, for example:

      i) First Responder Agencies (Police, Fire, Emergency Management)

      ii) Law Enforcement Support Agencies

      iii) Federal Agencies

      iv) CIKR Representatives

   e) Timelines are met.

   f) Log is updated as the investigation progresses, through final disposition.

INTELLIGENCE

Criminal Intelligence is defined as data that has been evaluated to determine:

1) It is relevant to both the identification of and the criminal activity engaged in by an individual or organization which is reasonably suspected of involvement in criminal activity, and
2) It meets the WSFC's criminal intelligence system submission criteria.

INTELLIGENCE CRITERIA

All intelligence collected by the WSFC shall meet the following criteria:

1) Reasonable suspicion that the individual or organization is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity – i.e., have a clearly defined criminal nexus.

   a) Reasonable Suspicion (Criminal Predicate) is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative

agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

2) Handled in accordance with applicable laws, rules, and regulations, to include 28 CFR Part 23.
   a) Criminal intelligence shall not be collected or maintained regarding the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.
   b) Shall not include any criminal intelligence that has been obtained in violation of any applicable Federal, State, or local law or ordinance.

INTELLIGENCE COLLECTOR

The Intelligence Collector (e.g., Officer, Detective) shall:

1) Rate the *source reliability*[i] using the following criteria:

Reliable	The reliability of the source is unquestioned or has been well tested in the past.
Usually Reliable	The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.
Unreliable	The reliability of the source has been sporadic in the past.
Unknown	The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

2) Rate the *content validity*, using the following criteria:

Confirmed	The information has been corroborated by an investigator or another independent, reliable source.
Probable	The information is consistent with past accounts.
Doubtful	The information is inconsistent with past accounts.
Cannot Be Judged	The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

3) The Intelligence Collector shall only enter collected intelligence into the database as directed by a WSFC Supervisor.

SUPERVISOR

1) Collected intelligence shall be reviewed and approved by ***two*** WSFC Supervisors to ensure that it meets collection requirements.
2) Supervisor shall determine/approve appropriate retention times for information:

a) 60 day working file

i) Working files consist of copies of reports, notes, and other documents used as investigative tools during investigative inquiries. These are considered official files for purpose of dissemination to outside agencies or individuals.

ii) A working file is used to develop a criminal nexus. Once a criminal nexus is established the file will be placed in a temporary file status.

iii) If no criminal nexus is found within 60 days the file shall be purged.

b) 1 year temporary file

i) Temporary file status is established when the individual or group involvement in criminal activity is questionable, and the reliability of the source or validity of the information is not able to be determined but the information appears to be significant enough to warrant storage.

ii) Temporary files shall be elevated and placed into permanent files when there are multiple reports on the same group or individuals.

iii) If no further information is found within one year the file shall be purged.

c) 5 year permanent file

i) Permanent files include individuals, groups, businesses, and organizations that have been positively identified and meet all WSFC intelligence criteria.

ii) Permanent files retention may be 'refreshed' with additional intelligence reports, thereby restarting the retention clock.

iii) If no new information is added after five years the file shall be purged.

3) After approval, the supervisor will direct the collector to enter intelligence in the database.

SECTION SUPERVISOR

The Section Supervisor tasked with primary follow-up responsibility shall, as appropriate, ensure that:

1) The Lead Investigator or Analyst is identified
2) Collaborate with other WSFC Sections
3) Follow-up is conducted with due diligence
4) Appropriate notifications are made to partners, for example:
   a) First Responder Agencies (Police, Fire, Emergency Management)
   b) Law Enforcement Support Agencies
   c) Federal Agencies
   d) CIKR Representatives
5) Timelines are met
6) Log is updated as the investigation progresses, through final disposition

REQUEST FOR PRODUCTS

An intelligence product is the systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being or known to be criminal in nature. WSFC products will be created utilizing a variety of sources, such as: open source, SARs, Information and Intelligence systems, Private Sector Partners, Informants, federal, state, and local databases.

1) Approval/Disapproval of Request
    a) The request for a WSFC product will be approved by the Duty Supervisor in consultation with the appropriate section supervisor, considering the following factors:
        i) Source of the request
            (1) Law Enforcement
            (2) Fire Department
            (3) Emergency Management
            (4) State Agency
            (5) Federal Agency
            (6) Private Sector
        ii) Type of product requested
            (1) Briefing (e.g., daily, event specific, threat)
            (2) Bulletins (e.g., Intelligence, Information, Officer Safety, Intelligence Warning)
            (3) Assessments (e.g., Threat, CIKR, Event planning)
            (4) Advisory Notifications
            (5) Request for Information
        iii) Target Audience
            (1) Law Enforcement/Public Safety
            (2) Emergency Management
            (3) Government
            (4) Private Sector
            (5) General Public
        iv) Current WSFC workload
    b) Duty Supervisor assigns request to the appropriate section supervisor
    c) Duty Supervisor updates Intake Log with current status.
2) Establishing priority and timelines
    a) Priority and timeline will be established in cooperation with the requestor and section supervisor.
    b) Priority for product request will be assigned based on the guidelines below:
        i) Priority 1: Time Sensitive

ii) Priority 2: By Specified Date

iii) Priority 3: Not Time Sensitive

c) Priorities are subject to change based on operational need.

3) Analytical products will be created utilizing established Law Enforcement Analytic Standards for Analytic Products/Processes[ii], to include:

a) Analytical products should be used to direct and support WSFC public and private sector partner operations. Analysis supports good resource management and is directly involved in creating situational awareness, in assisting in decision making, and in providing knowledge bases for trusted partners.

b) Analytic research shall be thorough and use all available sources. An analytic product shall contain all relevant data available through sources and means available to the analyst.

c) Raw data that has been obtained in violation of any applicable local, state, or federal law or ordinance shall not be incorporated into an analytic product.

d) Information collected from all sources shall be evaluated and designated for source reliability, content validity, and relevancy.

e) An analytic product shall be an accurate representation of the data. In cases where exculpatory data has been found along with proofs, both should be included.

f) Analyses shall utilize the best and most current computerized visualization and analytic tools available to the analyst. Visual aids shall be used to *enhance* products, and will not be produced without supporting documentation or explanation. Graphics are not analysis in and of themselves.

g) Analytic products shall always include analysis, assessments, integrated data, judgments, conclusions, and recommendations. Forecasts, estimates, and models shall be developed, where appropriate.

h) Every intelligence product shall clearly distinguish which contents are public domains or general unclassified information, what information is restricted, and what contents are the judgments or opinions of analysts and/or other professionals.

4) Templates and Format

a) Products will be completed utilizing the approved WSFC product templates, to include endnotes and/or footnotes referencing source documents.

b) The analyst will compile a product file, to include the following:

i) Source documentation

(1) Points of Contact

(2) Reports, and

(3) Hard copy of electronic sources

ii) Approval Coversheet

(1) Peer review

(2) Lead Analyst

(3) Section Supervisor

iii) Distribution List

iv) Final product (paper and electronic version)

v) Submit for review and approval

REQUEST FOR SERVICES

Washington State Fusion Center services include, but are not limited to: Intelligence Briefing, WSFC participation in a tabletop exercise, Investigative Support.

1) Approval/Disapproval of Request

a) The request for a WSFC service will be approved by the Duty Supervisor in consultation with the appropriate section supervisor and, as appropriate, the WSFC Director, considering the following factors:

i) Source of the request

(1) Law Enforcement

(2) Fire Department

(3) Emergency Management

(4) State Agency

(5) Federal Agency

(6) Private Sector

ii) Type of service requested

(1) Investigative support (e.g., surveillance, analytical research, warrant service)

(2) Briefing (e.g., threat, WSFC)

(3) Tabletop participation

(4) Meeting attendance

(5) Event planning participation

iii) Target Audience

(1) Law Enforcement/Public Safety

(2) Emergency Management

(3) Government

(4) Private Sector

(5) General Public

iv) Current WSFC workload

b) Duty Supervisor assigns request to the appropriate section supervisor

c) Duty Supervisor updates Intake Log with current status.

2) Establishing priority and timelines
   a) Priority and timeline will be established in cooperation with the requestor and section supervisor.
   b) Priority for the service request will be assigned based on the guidelines below:
      i) Priority 1: Time Sensitive
      ii) Priority 2: By Specified Date
      iii) Priority 3: Not Time Sensitive
   c) Priorities are subject to change based on operational need.
3) Analytical products/services will be created utilizing the following standards:
   a) Intelligence services should support WSFC public and private sector partner investigations and operations, to include prevention, protection, and preparedness efforts.
   b) Products may contain visual aids, but are only acceptable in addition to (not in place of) the written report/Presentation.
   c) Reports/presentations should contain conclusions and analytical comment when appropriate.
   d) Analytical products shall be accurate. Consumers must be able to rely on the data provided.
   e) Analytical products are time sensitive, and must reflect most timely information.
   f) Products must reflect all relevant data, to include supporting and derogatory information.
   g) Analysis should utilize all resources available to produce the best product possible in the time provided.
4) Templates and Format
   a) Products will be completed utilizing the approved WSFC product templates, e.g., WSFC PowerPoint Master, which includes reference source documents.
   b) The analyst will compile a product file, to include the following:
      i) Intake documentation
      ii) Source documentation
         (1) Points of Contact
         (2) Reports, and
         (3) Hard copy of electronic (web based) sources
      iii) Approval Coversheet (when appropriate)
         (1) Peer review
         (2) Lead Analyst
         (3) Section Supervisor
      iv) List or description of product consumers

v) Final product (paper and electronic version)

vi) Submit product for review and approval

OTHER

Requests for products and services that are not addressed in the sections above will be channeled through the Intake process and handled in consultation with the SAWC Duty Supervisor.

PRODUCT REVIEW AND APPROVAL

All WSFC Products must be reviewed and approved by a Supervisor prior to dissemination/final disposition. The following procedure will be used for quality control and product approval:

1) WSFC staff will request peer reviews of products and services, as appropriate, to evaluate products for:
   a) Grammar, punctuation, spelling
   b) Content
   c) Thoroughness
2) After peer review, bulletins and other analytical products will be forwarded to the Lead analyst for review, and will evaluate products for:
   a) Accuracy
   b) Thoroughness, to include appropriate contextual background
   c) Appropriate classification markings
   d) Format
3) After Lead Analyst review, or peer review of services, the Duty Supervisor will approve release and dissemination. The Duty Supervisor will evaluate products and services for:
   a) Civil liberties concerns
   b) Liability issues
   c) Overall content
4) Warning Bulletins and other products that are likely to have high visibility will be reviewed and approved by the Director of the WSFC before release for dissemination.[iii]

DISSEMINATION

Multi-directional information sharing is the key to prevention, protection, preparedness, and response. Dissemination is about getting the right information to the right people and places, having pre-established dissemination group lists of authorized recipients so that information can be shared in a timely manner.

All WSFC Personnel shall be familiar with information protection classifications utilized within the Center and the guidelines for disseminating such information. *See Appendix A for Dissemination Guidelines for Protected Information.*

DISSEMINATION LISTS

1) WSFC Sections shall collaborate with the Intake and Dissemination Officer to establish and maintain discrete distribution lists that accommodate the dissemination of intelligence and information, as detailed below:
   a) Regional and Statewide Support Section
      i) Criminal intelligence units and persons
      ii) Agency criminal investigators (Federal, State, Tribal, Local)
      iii) Local jurisdiction Fusion Center POC (Police, Fire, EM)[4]
   b) Critical Infrastructure Section
      i) State Homeland Security Advisor staff
      ii) Emergency management organizations and personnel
      iii) Transportation security organizations and personnel
      iv) Private Sector partners
      v) CIKR Liaisons
   c) Intelligence and Analysis Section
      i) Regional Intelligence Groups (RIGs) [i.e., analytical groups]
      ii) Fusion Liaison Officers (FLO) [Police and Fire]
      iii) Federal partners (examples: FBI, DHS, ATF, U.S. Attorney)
      iv) DHS components (examples: US Coast Guard, TSA, CBP, ICE, FEMA)
   d) Situational Awareness and Watch Center (SAWC)
      i) Government agency senior level leaders and managers of operational departments (for example: Chief WSP, Sheriffs, Police Chiefs, Fire Chiefs, Homeland Security Advisor, Director Emergency Management Department, Directors of EOCs)
         (1) Maintain dossiers for senior leadership in the State
      ii) Fire Departments and personnel

DISSEMINATION OFFICER

The dissemination function within the WSFC is handled by the Intake and Dissemination Officer, as approved by the SAWC Duty Supervisor. Dissemination of sensitive or other non-standard documents will be tailored at the discretion of the Director or supervisor to organizations and personnel with a need and right to know.

The Dissemination Officer will follow the procedures as described below when disseminating bulletins and other WSFC products:

1) Review all products and reports for proper labels, any special handling instructions and proper dissemination lists for the sensitivity of the content.

[4] Collaborate with WASPC, Washington State Fire Chief's Assoc, Emergency Management Assoc.

2) Certify and document that 28 CFR Part 23 documents containing information contributed by another agency is cleared by the originating agency for WSFC's re-dissemination to third parties. (i.e., Third Party Rule)
3) Log all dissemination from WSFC/SAWC. Log entries shall include:
   a) Date,
   b) Dissemination approved by,
   c) Person disseminating,
   d) Product or report type, and
   e) Destination agencies/recipients.
4) File all disseminated documents, including original and redacted versions, electronic and hard copy, in the WSFC filing systems.

REDACTION AND SANITIZATION

The Duty Supervisor is responsible for ensuring that products are appropriately redacted and sanitized as necessary. Drafters of products and reports may provide original full content versions of products and reports accompanied by redacted/sanitized versions.

For PCII-derived products, the WSFC's PCII Officer or Deputy PCII Officer shall review the redacted and sanitized version for dissemination, to ensure that PCII Program guidelines are followed.

The use of any classified material utilized for any WSFC products shall be cleared through the classifying agency. The date, time, and person clearing the product for dissemination shall be documented and stored with the file.

DISSEMINATION OF PROTECTED INFORMATION

Within the Information Sharing Environment of the WSFC, information will be designated as: Controlled Unclassified Information (CUI), Law Enforcement Sensitive (LES), and Protected Critical Infrastructure Information (PCII) to guide marking, safeguarding, and disseminating information.

The Duty Supervisor will ensure that information and intelligence has been appropriately redacted and sanitized according to its designation for the level of its dissemination. The original product, if designated as Intelligence or PCII, should include a 'tear line' (sanitized version) for CUI dissemination whenever possible.

Corrections additions or changes to information disseminated by the WSFC will be disseminated in the same manner as the original information in accordance with 28 CFR part 23.

APPENDIX A
DISSEMINATION GUIDELINES FOR PROTECTED INFORMATION

DISSEMINATION OF LAW ENFORCEMENT (CRIMINAL) INTELLIGENCE

The provisions of 28 CFR Part 23, which imposes conditions on the handling and dissemination of criminal intelligence information, govern law enforcement intelligence.

Law Enforcement Intelligence may be disseminated only to:

1) Individuals or agencies that have a *"right to know"* and *"need to know"*.
    a) "Right to know" means individuals or agencies that have the official standing and statutory authority to have access to the information.
    b) "Need to know" means individuals or agencies to which the information is pertinent and necessary for initiating, furthering or completing an investigation or legitimate law enforcement intelligence mission.
2) Law enforcement intelligence officers or agencies with a "right to know" and "need to know" in order to engage in cooperative and collaborative analytical work on a matter of mutual intelligence research interest.
3) Government personnel certified as civilian law enforcement intelligence analysts and as having the right and need to know law enforcement intelligence information to perform their mission.
4) Contractor personnel (such as analysts) who have a mission in direct support of an accredited law enforcement agency and are certified by that agency as having a "need to know' in order to perform their tasks.
    a) The sponsoring agency for such contractors must execute a confidentiality agreement that designates by name each contractor who is granted access to sensitive information in order carry out the sponsoring agency's mission.
        i) Among other provisions, confidentiality agreements should specify the limits and conditions of contractor access and when access should terminate.
    b) Each contractor working with law enforcement sensitive intelligence should also personally sign a confidentiality agreement.
        i) **Note:** A contractor authorized for access under a Confidentiality Agreement may not share law enforcement intelligence or information to which he or she has access with managers or other officers within their company who do not have similarly documented access authority.
5) Non-law enforcement government personnel so long as such personnel have a legitimate right and need to know the content of the intelligence to perform their mission. There are two circumstances for granting access:
    a) When law enforcement information or intelligence is received that points to an imminent threat to life and property. Such information should be released to all government

personnel who have a need to know the information in order to prevent or prepare to respond to the threat.

b) When non-law enforcement personnel have missions, such as homeland security or certain public safety missions that justify their access to law enforcement intelligence information. In such cases, the non-law enforcement agency normally will be required to execute a Memorandum of Understanding with a law enforcement agency outlining the conditions of access and use of the information to be shared.

   i) The non-law enforcement intelligence agency must also execute a confidentiality agreement naming all personnel who are to be granted access.

   ii) Each non-law enforcement government person granted access should execute a confidentiality agreement. Confidentiality agreements should specify:

      (1) The conditions and limits of access,

      (2) How information/intelligence to which they are granted access may be used, and

      (3) The time or conditions when access will be terminated.

THIRD PARTY DISSEMINATION RESTRICTION

An "original document" or "original" information obtained by one law enforcement agency from another law enforcement agency may not be released for dissemination to any other "third party agency" without the permission of the originating agency.

DISSEMINATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)[5]

The May 2008 Presidential Memorandum on the *Designation and Sharing of Controlled Unclassified Information* (CUI) defines CUI as the categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is:

- Pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, or
- Under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Previously, this information was referred to generally as Sensitive But Unclassified (SBU).

The National Archives and Records Administration is developing and will issue CUI policy standards and implementation guidance including appropriate recommendations to State, local, tribal, private sector, and foreign partner entities for implementing the CUI Framework.

Until CUI policy guidance and recognized standards for CUI markings including "safeguarding" and "dissemination" is developed by the Executive Agent, the WSFC will protect CUI utilizing guidance for safeguarding Sensitive But Unclassified (SBU)/For Official Use Only (FOUO) information.[6]

[5] Reference: Protected Critical Infrastructure Information Program Best Practices Series, June 2008

[6] Source: Safeguarding Classified and Sensitive Unclassified Information; Reference Guide for State, Local, Tribal and Private Sector Programs

WSFC policies will be reviewed and revised as appropriate once CUI standards are published.

CUI HANDLING REQUIREMENTS

CUI MARKING

Information determined to be CUI will be sufficiently marked so that persons granted access to it are aware of its sensitivity and protection requirements. At a minimum, it is marked on the bottom of each page "CONTROLLED UNCLASSIFIED INFORMATION."

CUI ACCESS AND DISSEMINATION

A security clearance is not needed for access to CUI. Access to CUI data is based on a "need-to-know" as determined by the holder of the information. Where there is uncertainty as to a person's need to know, the holder should request dissemination instructions from their next-level supervisor or the originating activity.

CUI may be shared with other agencies, federal, state, tribal, private sector, or local government and law enforcement officials, provided a need-to-know has been established and the information is shared in the furtherance of an official government activity, to include homeland defense, and no dissemination restrictions have been cited by the originator.

1) When discussing CUI over a telephone, use of the STU-III or STE is encouraged, but not required.
2) CUI may be transmitted via non-secure fax machine, although the use of a secure fax is encouraged. Where a non-secure fax machine is used, ensure that a recipient is present at the time of the fax and that the materials faxed will not be left unattended or subject to unauthorized disclosure.
3) CUI may be transmitted over official e-mail channels. However, it shall not be sent to personal e-mail accounts. For added security when transmitting CUI by e-mail, password-protected attachments may be used with the password transmitted or otherwise communicated separately.
4) Do not enter or post any CUI on any public website.
5) CUI may be mailed by regular U.S. Postal Service first class mail or any commercial mailing service.

CUI STORAGE

If in use, CUI materials will be protected from casual observation or access. When unattended, CUI will be kept, at a minimum, stored in a locked file cabinet, desk drawer, furniture compartment, or other locked compartment or a locked room with controlled and restricted access. Information can also be stored in a room or area that has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without the need-to-know, such as a locked room or an area where access is controlled by a guard, cipher lock, or card reader.

CUI DESTRUCTION

Hardcopy CUI materials are to be disposed of by destroying them by shredding, burning, pulping, or pulverizing beyond recognition and reconstruction. After appropriate destruction, materials may be disposed of with normal waste in regular trash or recycling receptacles.

Electronic storage media shall be sanitized appropriately by overwriting (additional data is written over the information on the hard drive), or degaussing (information is scrambled.)

Paper products or electronic media containing CUI will not be disposed of in regular trash or recycling receptacles unless the materials have been destroyed as specified above.

INCIDENT REPORTING

Compromise, suspected compromise, and suspicious or inappropriate requests for CUI shall be reported to the originator of the information.

DISSEMINATION OF PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII)[7]

Protected Critical Infrastructure Information (PCII) is governed by the provisions of the Critical Infrastructure (CII) Act of 2002 and implementing Regulation at 6 CFR Part 29 that imposes conditions on the handling and dissemination of Protected Critical Infrastructure Information.

Designees (Federal, State, and local government entities) and authorized PCII users may disseminate PCII in their possession provided they ensure that the person to whom they are disseminating PCII meets all the access requirements set forth below. Authorized Users must transmit PCII in accordance with the procedures set forth in the PCII Program's Day-to-Day Operations Best Practices, maintained by the CIKR Supervisor/WSFC PCII Officer.

Before accessing PCII, an individual must meet the PCII Program Office's requirements, which include:

1) **Be an Individual Employee or Contractor for a Federal, State, or Local Government Entity.** *Members of the private sector, individual citizens, media, trade associations, and other private sector organizations cannot be PCII Authorized Users.*

2) **Be assigned Homeland Security Duties.**

3) **Complete PCII Training**

   In limited and exigent circumstances, PCII training can be accomplished expeditiously with the PCII Cover Sheet. These steps are outlined in more detail in the PCII Program Best Practices documentation that is maintained by the CIKR Supervisor/WSFC PCII Officer.

4) **Sign a Non-Disclosure Agreement (Non-Federal Employees Only).** PCII Program Best Practices documentation that is maintained by the CIKR Supervisor/WSFC PCII Officer.

5) **Be Certified by the PCII Program Office or the PCII Officer (Contractors Only).** Prior to accessing PCII, a contractor must be certified by either the PCII Program Office or a PCII Officer. Before or during participation in the PCII Program, the contractor must agree by contract to adhere to and implement PCII Program requirements. See section entitled "Contractor Certification" that provides additional detail about contractor certification and

[7] Reference: Protected Critical Infrastructure Information Program Best Practices Series, June 2008

the language to incorporate into the contract with the government agency in the PCII Program Best Practices documentation that is maintained by the CIKR Supervisor/WSFC PCII Officer.

6) **Have a Valid Need-to-Know.** Any individual accessing PCII must have a need to know for that particular PCII. Before disseminating PCII, the holder of PCII must determine whether the prospective recipient has a valid need-to-know the information. Although the determination of whether an individual or an organization has a valid need-to-know is a judgment call made on a case-by-case basis, the determination should be made based on whether the individual has homeland security duties and what the recipient intends to do with the PCII.

   a) Section 214 (a) of the CII Act lists the authorized uses of PCII (which includes use of PCII in work products) as:

      (1) Securing the critical infrastructure and protected systems

      (2) Analysis

      (3) Warning

      (4) Interdependency study

      (5) Recovery

      (6) Reconstitution

      (7) Another information purpose, including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland.

PCII DISSEMINATION REQUIREMENTS

1) Information submitted for protection under the CII Act may not be disseminated until it has been validated and properly marked as PCII.

2) The PCII Program Office or the Designee is authorized to provide access to PCII when it is determined that this access supports homeland security purposes as set forth in the CII Act.

3) The PCII Program Office or the Designee may provide PCII to Federal departments and agencies and to State and local government entities that have executed an MOA with the PCII Program Manager and have met the minimum requirements of the PCII Accreditation Program.

4) The PCII PM or the Designee is responsible for tracking PCII initially provided to the Federal, State, or local government entity.

5) Reference the PCII Program Best Practices documentation maintained by the WSFC CIKR Supervisor/WSFC PCII Officer for more information.

THIRD PARTY DISSEMINATION RESTRICTION

State and local government employees and contractors receiving PCII may not share it with any parties that have not been authorized by the PCII PM or the Designee.

If State and local government employees and contractors want to share PCII with unauthorized users, the users must:

1) Become authorized or the employee must obtain the express approval of the PCII PM or the Designee to share the PCII with an unauthorized user.
2) The PCII PM generally will not grant such approval without the written consent of the submitter.

---

[i] Information to be retained in the criminal intelligence file will be evaluated and designated for reliability and content validity, based on LEIU standards. http://fas.org/irp/agency/doj/lei/app.pdf

[ii] Standards based on "Law Enforcement Analytic Standards" published by the United States Department of Justice and International Association of Law Enforcement Intelligence Analysts (IALEIA).

[iii] Warning Bulletins are issued when there are credible reports or analytical indications of a specific or imminent threat to security and safety. Warning Bulletins are advisory in nature. They provide political leaders, departmental decision-makers and agency contingency planners with an advanced indication and description of a threat – giving leaders and decision makers the opportunity to consider options, such as setting in motion contingency plans, stepping up prevention operations, and deciding if operational warning is warranted.

Washington State Fusion Center
Privacy Policy

Purpose Statement

The purpose of the Washington State Fusion Center (WSFC) Privacy Policy is to ensure that the collection, evaluation, analysis and dissemination of information and intelligence data regarding criminal activity is conducted in a manner that protects public safety while protecting civil rights, civil liberties and personal privacy. This policy has the express purpose of fulfilling that mission by ensuring strict adherence to all applicable federal and state constitutional rights, statutory, and regulatory protections while:

- Protecting the integrity of systems for the observation and reporting of terrorism-related criminal activity and information;
- Encouraging individuals or community groups to trust and cooperate with the justice system;
- Promoting governmental legitimacy and accountability; and
- Making the most effective use of public resources allocated to public safety agencies.

Policy Applicability and Legal Compliance

1. The WSFC will adopt a Concept of Operations and Standard Operating Procedures that are consistent with the provisions of this privacy policy, as well as all applicable state and federal constitutional rights and statutes and regulations, including 28 CFR Part 23.

2. All personnel assigned to the WSFC, including private contractors and authorized participating agencies will comply with the WSFC's privacy policy while carrying out WSFC responsibilities at the direction of the WSFC and its representatives, or otherwise acting within the scope of their assigned WSFC duties. Nothing in this policy is, however, meant to preempt superseding federal or state laws, regulations, or constitutional provisions.

3. The WSFC will make this policy available on-line to personnel and authorized users and will provide a printed copy of this policy to all WSFC personnel, who will be required to sign both a written acknowledgement of receipt of this policy, as well as a written agreement to comply with the privacy policy.

4. It is the policy of WSFC, where relevant and appropriate, to provide the enhanced protections of the Information Sharing Environment (ISE) for terrorism-related information to all personal identifiable information shared by WSFC with authorized participating agencies.

Governance and Oversight

1. The WSFC Executive Board is responsible for approving WSFC policies and procedures and ensuring that audit and oversight mechanisms are in place to ensure compliance. The Director of the WSFC is responsible for approving an Interim Privacy Policy until the Executive Board can approve a final policy. The Director is also responsible for the day-to-day operations of the WSFC, including enforcement of this privacy policy. The Director will appoint a designated and trained internal Privacy and Civil Liberties Officer to monitor compliance with this policy and act as a resource. This person will also act as the liaison for the Information Sharing Environment.

2. The WSFC Executive Board will establish a privacy oversight mechanism to review and make recommendations regarding WSFC privacy policy and procedures to ensure that appropriate revisions are made in response to changes in technology, policy, or law, and to oversee a minimum of an annual audit of WSFC operations to determine compliance with this policy.

3. Personnel, contractors and others who fail to abide by provisions of this policy applicable to them may be denied access to information sharing mechanisms of the WSFC or other appropriate sanction as determined by the WSFC Executive Board, including potential termination of participation with the WSFC.

Information Collection, Retention and Dissemination Standards

1. The WSFC will only collect, analyze, retain or disseminate information that was lawfully obtained and is relevant to the investigation and prosecution of suspected criminal activity, threats to public safety or other legitimate criminal justice purpose. For purposes of this policy, "information" includes any information or intelligence "about an identifiable individual or organization that the WSFC may legally obtain, review, retain, etc., such as suspicious activity reports (SARs) and other tips and leads information, criminal histories, incident reports, public records, etc." See Appendix C for SAR Guidelines that the WSFC will follow for this type of information.

2. The WSFC will not seek, retain or disseminate any information about individuals or organizations solely on the basis of their race, ethnicity, gender, age, sexual orientation or disability. This protection also extends to religious or political activities and beliefs. Since government actions can unintentionally inhibit the exercise of state and federal constitutional rights, this policy further specifically prohibits the collection, retention or dissemination of personal identifying information (PII) about an individual's non-criminal participation in protected First Amendment activities such as speech, assembly and petition which may take various forms to include protests, rallies, etc., without a legitimate law enforcement purpose meeting the standards and procedures of this policy.

3. Any criminal information related to protected First Amendment activities shall be first reviewed by the Privacy and Civil Liberties Officer and then specifically approved by the WSFC Director prior to retention or dissemination. In addition to the applying the criminal standard, the review and approval shall ensure that any misdemeanor criminal conduct alleged has a legitimate law enforcement purpose and is relevant to the core responsibilities of the WSFC.

4. When the decision to retain information is made, it will be labeled, stored and disseminated in a manner that:

   - Protects the right of privacy and civil liberties
   - Protects confidential sources and methods
   - Provides all legally required protections

   Information will be assessed upon receipt to determine its nature, usability, and quality and labeled to indicate to the user the category of information, the nature of the source, and confidence levels, where appropriate. The labeling of retained information will be reevaluated when new information is collected that has an impact on the confidence in previously retained information.

5. All personal identifiable information collected by WSFC and shared through the ISE, shall include, where relevant and appropriate, the name of the originating agency, the information system from which the information is provided, the date the information was collected, and the title and contact information for the person in the originating agency to whom inquiries should be directed.

6. All personal identifiable information with access restrictions will be so labeled when it is disseminated to reflect limitations on access and sensitivity of disclosure. Those limitations will be updated when the WSFC receives new information that impacts those access restrictions or there is a change in the use of the information affecting access or disclosure limitations.

7. Information gathering and investigative techniques used by the WSFC and information originating agencies shall be in compliance with and will adhere to applicable constitutional provisions, statutes and regulations. Intelligence information shall be collected, stored and disseminated in compliance with 28 CFR Part 23 (Appendix A), and the LEIU Criminal Intelligence File Guidelines (Appendix B), including the Third Party Rule, as well as all applicable federal and state constitutional provisions.

Information Quality Assurance

1. The WSFC will make every reasonable effort to ensure that, prior to retaining or disseminating information, the information is accurate and complete, and includes the context in which the information was received. This will include labeling

information to identify, where relevant and appropriate, its source and level of quality, including confidence in the information (source reliability and content validity), accuracy, completeness, currency, and whether it has been verified.

2. The WSFC will investigate and correct or delete, in a timely manner, any alleged errors and deficiencies in the information the fusion center has retained or disseminated, whether by internal discovery or external complaint of error. If the WSFC discovers that information it has received from an originating agency is inaccurate or otherwise unreliable, it will notify the originating agency in writing, including electronic notification. This will include written (electronic) notification to any individual or entity that the WSFC knows has received the incorrect information. To facilitate these notifications, the WSFC will develop a computer system that tracks the dissemination of information and intelligence and any corrections (including related new information) or deletions.

3. All criminal intelligence information will be electronically marked with its purge date upon entry into a criminal intelligence database and validated for retention purposes or purged at least every five years. Information and intelligence that is no longer relevant, including criminal intelligence information no longer eligible to be retained under 28 CFR Part 23, will be electronically purged, returned to the originating agency as appropriate, or otherwise archived as required by law. Source agencies will not be notified of pending purge dates.

4. Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match If the information is insufficient to allow merging of the record, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

5. Records will be provided to requestors, unless exempt from disclosure under chapter 42.56 RCW Washington Public Records Act. When information is exempt from disclosure and an individual or group has a complaint or other objection to the accuracy of information regarding that person or group, the WSFC will acknowledge the complaint and: (a) if the information originates from the WSFC, the WSFC will investigate the complaint and either conform the information, correct it, or remove it from an information database; or (b) if the information does not originate from the WSFC, the complaint will be referred to the source agency for investigation. A record of all such requests, and any confirmation or correction/removal action taken, will be maintained by the WSFC. Pending investigation and resolution, the information complained about will not be disseminated by the WSFC.

6. The WSFC Director will be responsible to ensure that all complaints about information originating from the WSFC are fully investigated, appropriate action is taken in response to the investigation, and notification of resolution is made to the complainant. Such notification will include the procedure to appeal the Director's determination, as provided by the Washington Public Records Law.

Information Security

1. Credentialed, role-based criteria are crucial for information security and privacy protections. Access limitations, along with an inquiry log and audit trail maintained by WSFC for WSFC databases, will identify and limit:

   - The authorized user making an inquiry, the subject of the inquiry, and the information that the user has accessed;
   - Whether the authorized user can enter, change, delete or print information or took any of these actions; and
   - To whom information can be disseminated and under what circumstances.

   Only qualified individuals with the appropriate credentials and training will analyze information acquired or accessed by the center.

   These restrictions will be reevaluated whenever the WSFC receives additional information which merits a change in information restrictions, such as a national security classification.

2. Access to or disclosure of records collected or retained by the WSFC will be provided only to persons who are authorized to have such access in accordance with all applicable federal and state laws, and in furtherance of legitimate public safety purposes. All WSFC personnel, including contractors will undergo a full background investigation in addition to a security clearance investigation for those individuals having access to classified information.

3. Any information disseminated by the WSFC will contain dissemination restriction language appropriate for the particular type of material, such as "law enforcement sensitive," and "third-party" rule restrictions.

4. The WSFC Director shall appoint a security officer. The Security Officer shall receive appropriate training and shall work in concert with the FBI security manager to ensure compliance with information security procedures. These security procedures will include:

   - Secure internal and external safeguards against network intrusions;
   - Information will be stored so that it cannot be modified, accessed, destroyed or purged except by authorized personnel with the appropriate background investigations and security clearances; and
   - Appropriate physical security safeguards are in place to protect information.

5. Risk and Vulnerability Assessments will be stored separately from publicly available data.

6. Unless legal or security restrictions prohibit it, or unless it would compromise a legitimate law enforcement purpose, such as an ongoing investigation, source or method, etc., (a) the WSFC will follow RCW 42.56.590 in the event of a data security breach; and (b) the WSFC will protect sensitive government records and private information consistent with chapter 42.56 RCW,, the Washington Public Records Act.

Accountability and Enforcement

1. The public has a right to know the information and privacy safeguards of the WSFC. The WSFC's privacy policy will be made available upon request and will be posted on a public web portal to be developed.

2. To enable oversight and enforcement of these provisions, the WSFC will implement a computerized record system that maintains an audit trail of all access and dissemination of WSFC records. This audit trail will be maintained a minimum of five years.

3. In addition to being provided a copy of this policy, all WSFC personnel will be required to participate in training regarding adhering to this policy. This training will include, at a minimum, the purpose of the policy, substance and intent of the provisions of the policy, impact of infractions, and possible penalties for violations. Personnel authorized to share personal identifiable information in the ISE shall receive specialized training regarding WSFC requirements and policies for the collection, disclosure and use of this information. User agencies, not the WSFC, are responsible for providing appropriate training, such as how to handle intelligence or law enforcement sensitive information, e.g., the Third Party Rule, to their personnel submitting information to WSFC or who have access to protected information disseminated by WSFC.

4. All personnel assigned to the WSFC have a duty to uphold the privacy and civil liberties protections in this policy, to cooperate with audits and reviews by oversight officials with responsibility for information sharing, and to report violations of WSFC policies related to protected information to the WSFC Privacy and Civil Liberties Officer, who shall serve as the initial receiving point for inquiries and complaints about privacy and civil liberties concerns, and who will receive reports of suspected or confirmed violations. The WSFC Director is responsible for ensuring adherence to this policy.

5. The WSFC Executive Board will ensure that an annual audit is conducted to review compliance with WSFC information systems requirements and the WSFC Privacy Policy. The panel will report its findings to the Executive Board along with any

recommendations for corrective action or policy modification. If suggestions for policy modification are approved, the Policy will be updated annually to reflect those suggestions and any other modification required in response to changes in applicable law, technology, or the purpose and use of information systems.

Appendix A – 28 CFR Part 23

See:
http://www.iir.com/28cfr/pdf/ExecOrder12291_28CFRPart23.pdf.

and
http://www.iir.com/28cfr/pdf/1993RevisionCommentary_28CFRPart23.pdf.

Appendix B- LEIU File Guidelines

See:
http://it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.

Appendix C- SAR Guidelines

The WSFC will incorporate the gathering, processing, reporting, analyzing, and sharing of Suspicious Activity Reporting (SAR) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as the privacy, civil rights, and civil liberties of individuals. In addition to those protections, the following provisions uniquely apply to SAR information and are derived from the Program Manager's Office of the Information Sharing Environment (PM-ISE) regarding the National SAR Initiative operated under the auspices of that office.

Information Collection, Retention and Dissemination Standards

1. All WSFC personnel will receive training to recognize behaviors and other indicators of criminal activity related to terrorism that also includes training to avoid inappropriate behavior in violation of this policy such as racial, religious or ethnic profiling.

2. Upon receipt of SAR information from a source agency that has processed the information in accordance with WSFC criteria, designated WSFC personnel will:

    - Personally review and vet the SAR information and provide the two-step assessment set forth in the ISE-SAR Functional Standard to determine whether the information qualifies as an ISE-SAR (alternatively, WSFC personnel will confirm that such an assessment has been conducted by an authorized source agency).
    - Enter the information following Information Exchange Package Documentation (IEPD) standards and code conventions to the extent feasible.
    - Provide appropriate labels as required under #3 below.
    - Post the ISE-SAR to the FC's shared space.
    - Notify the source agency that the SAR has been identified as an ISE SAR and submitted to the shared space.

3. The WSFC will ensure that certain basic and special descriptive information is entered and electronically associated with ISE-SAR information, including:

    - The name of the source agency.
    - The date the information was submitted.
    - The point-of-contact information for SAR-related data.
    - Information that reflects any special laws, rules, or policies regarding access, use, and disclosure.

4. Information provided in the ISE-SAR shall indicate, to the maximum extent feasible and consistent with the *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR) Version 1.0* (ISE-FS-200):

    - *The nature of the source*: anonymous tip, confidential source, trained interviewer or investigator, written statement (victim, witness, other), private sector, or other source.
    - Confidence, including:
        The reliability of the source:
        - *Reliable—the source has been determined to be reliable.*
        - *Unreliable—the reliability of the source is doubtful or has been determined to be unreliable.*
        - *Unknown—the reliability of the source cannot be judged or has not as yet been assessed.*

        The validity of the content:
        - *Confirmed—information has been corroborated by an investigator or other reliable source.*
        - *Doubtful—the information is of questionable credibility but cannot be discounted.*
        - *Cannot be judged—the information cannot be confirmed.*
    - Due diligence will be exercised in determining source reliability and content validity. Information determined to be unfounded will be purged from the shared space.
    - Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or validate it through their own investigation.

5. At the time a decision is made to post ISE-SAR information to the shared space, WSFC personnel will ensure that the ISE-SAR information is labeled, to the maximum extent feasible and consistent with the ISE-SAR FS, to reflect any limitations on disclosure based on sensitivity of disclosure (dissemination description code), in order to:

    - Protect an *individual's* right to privacy, civil rights, and civil liberties.
    - Protect *confidential* sources and police undercover techniques and methods.
    - Not *interfere* with or compromise pending criminal investigations.
    - Provide *any* legally required protection based on an individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The WSFC will share ISE-SAR information with authorized nonfusion center agencies and individuals only in accordance with established WSFC policy and procedure.

7. Notice will be provided through data field labels or narrative information to enable authorized users to determine the nature of the protected information in the shared space and how to handle the information in accordance with applicable legal requirements, including any restrictions based on information security or classification.

Information Quality Assurance

1. The WSFC will ensure that source agencies assume primary responsibility for the quality and accuracy of the SAR data collected by the WSFC. The WSFC will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if SAR information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

2. The WSFC will make every reasonable effort to ensure that SAR information collected and ISE-SAR information retained and posted to the shared space is derived from dependable and trustworthy source agencies and is as accurate, current, and complete as possible.

3. At the time of posting to the shared space, ISE-SAR information will be labeled according to the level of confidence in the information (source reliability and content validity) to the maximum extent feasible.

4. The labeling of ISE-SAR information will be periodically evaluated and updated in the shared space when new information is acquired that has an impact on confidence in the information.

5. Alleged errors or deficiencies (misleading, obsolete, or otherwise unreliable) in ISE-SAR information will be investigated in a timely manner and any needed corrections to or deletions made to such information in the shared space.

6. ISE-SAR information will be removed from the shared space if it is determined the source agency did not have authority to acquire the original SAR information, used prohibited means to acquire it, or did not have authority to provide it to the WSFC or if the information is subject to an expungement order in a state or federal court that is enforceable under state law or policy.

7. The WSFC will provide written notice (this would include electronic notification) to the source agency that provided the SAR and to any user agency that has accessed the ISE-SAR information posted to the shared space when ISE-SAR information posted to the shared space by the WSFC is corrected or removed from the shared space by the WSFC because it is erroneous or deficient such that the rights of an individual may be affected.

Sharing and Disclosure

1. Credentialed, role-based access criteria will be used, as appropriate, to determine which system users will be authorized to view privacy fields in ISE-SAR information in response to queries made through a federated ISE-SAR search.

2. Unless an exception is expressly approved by the PM-ISE, the WSFC will adhere to the Functional Standard for the ISE-SAR process, including the use of the ISE-SAR IEPD reporting format, EE Initiative-approved data collection codes, and ISE-SAR information sharing and disclosure business rules.

3. ISE-SAR information retained by the WSFC and entered into the WSFC's shared space will be accessed by or disseminated only to persons within the WSFC or, as expressly approved by the PM-ISE, users who are authorized to have access and need the information ***for specific purposes authorized by law***. Access and disclosure of personal information will be allowed to agencies and individual users only for legitimate law enforcement and public protection purposes and for the performance of official duties in accordance with law.

Appendix D- Definitions

The following is a list of primary terms and definitions used throughout the WSFC Interim Privacy Policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

Agency—Agency refers to the WSFC and all agencies that access, contribute, and share information in the [name of agency]'s justice information system.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights—the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Credentials—Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures.

Data Protection—Data protection encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Notification—Notice that is provided by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Logs—The recording a sequence of activity on a system Logs are a necessary part of an adequate security system because they help ensure that data is properly tracked and that only authorized individuals are getting access to the data. See also Audit Trail.

Personal Identifiable Information—Personal identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to identify a unique individual.

Privacy—Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the

agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, it includes applicable state and tribal constitutions and state, local, and tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency/center in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—Internal procedures to address complaints from persons regarding protected information about them that is under the agency's/center's control.

Retention—Refer to Storage.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Security—Security refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

   Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity—Suspicious activity is defined as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR)—Official documentation of a suspicious activity. At the federal level, there are two types of SAR information: 1) Information Sharing Environment SAR information that pertains to terrorism information; and 2) Banking Secrecy Act SAR information that pertains to suspicious banking activity and is required to be completed by financial institutions. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of IRTPA, all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational

terrorism, (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Weapons of Mass Destruction (WMD) information is a defined sub-category of terrorism information.

Terrorism-Related Information—In accordance with IRTPA, as amended by the 9/11 Commission Act, August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads may include suspicious incident report (SIR) information, suspicious activity report (SAR) information, and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information should maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information raises some suspicion but may be based on a level of suspicion that is less than "reasonable suspicion" and, without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.