

Guideline 9

Ensure appropriate security measures are in place for the facility, data, and personnel.

Security

Justification

Security pertains to information, documents, databases, facility, and personnel and includes measures such as authorization, encryption, access control, and confidentiality. In determining how most appropriately to protect data, there are many policy and technical issues for data owners to consider. It is important that policy issues be decided upon before technical issues are developed.

The private sector is affected by market forces, shareholder value, and various rules and regulations regarding the sharing and storage of information, including antitrust laws and the Freedom of Information Act (FOIA). The Homeland Security Act of 2002 states that the Critical Infrastructure Information Act grants an exemption from FOIA for the U.S. Department of Homeland Security (DHS) when private sector companies provide critical infrastructure information for the purposes of homeland security-related issues.

In addition, the Critical Infrastructure Information Act provides for the protection of critical infrastructure information submitted to DHS and subsequently shared with local and state agencies for the purposes of ensuring the resilience of critical infrastructure operations or in furtherance of an investigation of a criminal act.⁵⁰ When private sector entities submit critical infrastructure information to the fusion center, the center must ensure the information is protected from unauthorized disclosure. Fusion center leadership should be aware of local, state, and federal laws regarding the release of information, including state sunshine laws and FOIA.

Facility and personnel security should also be a part of the center's security plan. Appropriate security clearances should be obtained for personnel within the fusion center and key decision makers who need access. Security plans should be marked, handled, and controlled as sensitive but unclassified information. Some questions to consider when developing a security policy and plan include:

⁵⁰ Homeland Security Act of 2002, Critical Infrastructure Information, www.dhs.gov/interweb/assetlibrary/CII_Act.pdf.

- Who does the data owner want to have access?
- How should users access the data?
- What access methods are necessary for the users' jobs?
- Should audits be used to ensure proper use of data?
- Should centers conduct background checks on personnel?
- What security needs exist for the facility?
- What security is needed for the data?
- Should a system-logging mechanism be used?

Issues for Consideration

When developing security protocols, consider:

- Adopting established models for secure information and intelligence sharing, such as Regional Information Sharing Systems (RISS), Law Enforcement Online (LEO), Regional Data Exchange (R-DEX), and Homeland Security Information Network (HSIN).
- Addressing limited/restricted access, authorization, authentication, and encryption.
- Applying security policies to both physical and electronic forms of information.



- Using the *Applying Security Practices to Justice Information Sharing* document.
- Determining access levels and maintaining a policy on the level of information released.
- Verifying access based on criteria established by governance structure.
- Creating a form to be submitted by the agency authorizing access/supervisory approval.
- Conducting background checks on personnel.
- Utilizing local or state law enforcement agency background check standards on public safety and private sector participants, to the extent permissible by state law.
- Clearly defining in the Memorandum of Understanding (MOU) all background check criteria or guidelines to law enforcement, public safety, and private sector partners.
- Consulting the *National Criminal Intelligence Sharing Plan* (NCISP) (Recommendation 28) when developing a background check policy.
- Using applicable security guidelines for access control.
- Providing relevant security clearances.
- Creating and providing a training component on center security protocols.
- Utilizing relevant local, state, and federal building security requirements.
- Utilizing relevant portions of 28 CFR Part 23 as it relates to security.
- Appointing a privacy officer as a central point for compliance and oversight.

Centers may also consider maintaining a security officer who is responsible for evaluating and providing information about the security program to management and communicating security requirements and concerns to the organization. The security officer conducts security training and awareness and prepares a policy on security. Any breach issues would be reported to and investigated by the security officer. The security officer should also coordinate background checks on center personnel. Background checks are important because, although the information and intelligence disseminated by the fusion center may be unclassified, it is still sensitive, and therefore all appropriate methods of information protection should be undertaken, including background checks. The NCISP states that “background requirements for access to the nationwide sensitive but unclassified communications capability by law enforcement personnel shall be consistent with requirements applied to the designation and employment of sworn personnel, as set by the participating state or tribal government.”⁵¹ Consideration should be given to colocating with other intelligence centers, such as High Intensity Drug Trafficking Areas (HIDTA) or other law enforcement facilities, in order to share security responsibilities.

Applying Security Practices to Justice Information Sharing provides details on how to safeguard critical elements of information sharing initiatives, as well as the infrastructure and integrity of data, systems, facilities, and personnel. According to

the document, the following issues should be considered when developing and adhering to security policies:

- Identify potential physical threats to departmental computer systems and networks.
- Establish policies and procedures to thwart potential physical threats.
- Conduct audits to monitor employee compliance with department policies and procedures.
- Consider including the following physical security policies in the organization’s overall security policy:
 - ✓ Identify unauthorized hardware attached to the department computer system; make routine checks of system hardware for unauthorized hardware.
 - ✓ Limit installation of hardware and software owned by employees on department desktop workstations.
 - ✓ Identify, tag, and inventory all computer system hardware.
 - ✓ Conduct regular inspections and inventories of system hardware.
 - ✓ Conduct unscheduled inspections and inventories of system hardware.
 - ✓ Implement policies that instruct employees/users on how to react to intruders and how to respond to incidents where an intrusion has been detected.
- Require background checks on all employees every five years.

Federal regulation 28 CFR Part 23 is a guideline for law enforcement agencies that operate federally funded, multijurisdictional criminal intelligence systems, and it provides the following guidelines regarding security:

- The database, manual or electronic, shall be located in a physically secured area that is restricted to designated authorized personnel.
- Only designated authorized personnel will have access to information stored in the database.
- All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility and physical location housing the database.
- All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- All hard-copy submissions and/or manual files will be secured by lead agency-designated authorized personnel when not being used and at the end of each shift.
- Employment policies and procedures for screening/rejecting, transferring, or removing personnel having direct access will be adopted.
- When direct remote terminal access is authorized by participating agencies, policies and procedures addressing the following additional security measures shall be adopted:
 - ✓ Identification of authorized remote terminals and security of terminals.

⁵¹ NCISP, pp. 24-25.

- ✓ Identification and verification of an authorized access officer (remote terminal operator).
- ✓ Identification of levels of dissemination of information as directed by the submitting agency.
- ✓ Rejection of submissions unless critical data fields are completed.
- ✓ Technological safeguards on access, use, dissemination, and review and purge.
- ✓ Physical security.
- ✓ Training and certification of participating agency personnel.
- ✓ Audits and inspections of participating agencies, including file data-supporting submissions, security of access terminals, and policy-and-procedure compliance.
- ✓ Documentation for audit trails of the entire operation.

Available Resources on Fusion Center CD

- *Applying Security Practices to Justice Information Sharing*, <http://it.ojp.gov/documents/asp/introduction/index.htm>
- Critical Infrastructure Information Act of 2002, www.dhs.gov/interweb/assetlibrary/CII_Act.pdf
- National Institute of Standards and Technology (NIST) template and example policies, <http://csrc.nist.gov/fasp>
- *Safeguarding Classified and Sensitive But Unclassified Information, Reference Booklet for State, Local, Tribal, and Private Sector Programs*, U.S. Department of Homeland Security, May 2005