

# Guideline 14

Offer a variety of intelligence services and products to customers.

## Intelligence Services and Products

### Justification

The majority of the initiatives reviewed during the focus group's processes operate 24 hours a day, 7 days a week and act as a clearinghouse for information and/or intelligence sharing. The intelligence process acts as the framework but does not limit information sharing to intelligence product dissemination. As such, personnel utilize the intelligence process while producing analytical services, such as crime-pattern analysis, association analysis, telephone-toll analysis, flowcharting, financial analysis, and strategic analysis. Fusion centers should take into account the needs and requirements of their respective jurisdictions when producing products and services.

As a result of sharing information throughout the intelligence process, the initiatives provide an array of intelligence products, such as intelligence reports, briefs, threat assessments, charts, graphs, and mapping. Thus, it is important that center personnel, especially analysts, be familiar with computer applications that have information storage capabilities which allow the user to sort, query, and filter information; applications for presenting information; and applications for linking and flowcharting.

Some initiatives have compartmentalized their operations by creating divisions, such as investigations, intelligence, and administration. This structure may assist in identifying and assigning responsibilities, as well as holding personnel accountable. It is important to know who the program's customers are and what types of services and products they need.

### Issues for Consideration

It is recommended that law enforcement intelligence programs produce both strategic and tactical products to support the mission and priorities of the center. A major purpose of intelligence analysis is management decision making. Consider providing the following services and products:

- Investigative and tactical response
- Proactive strategic analysis

- Intelligence support for investigations
- Visual investigative analysis
- Alerts and notifications
- Deconfliction
- Target identification
- Critical infrastructure analysis
- Training opportunities
- Geospatial imaging
- Criminal backgrounds and profiles
- Case correlation
- Crime-pattern analysis
- Association, link, and network analysis
- Telephone-toll analysis
- Flowcharting
- Financial analysis
- Intelligence reports and briefings
- Threat assessments
- Terrorism calendar

Centers should prioritize their intelligence function, based on specific threats in their jurisdictions/regions, and integrate intelligence-led policing to support customer needs, define tasks, and prioritize functions. When specific threats are identified, centers should partner with agencies and organizations that can aid in analysis, e.g., computer analysis and forensic analysis. For example, if a government network has been hacked into, then computer resources from law enforcement and the private sector may help the investigation and analysis.

### Standards for Analytical Products

The *National Criminal Intelligence Sharing Plan* (NCISP) recommends that the agency chief executive officer and the manager of intelligence functions should "support the development of sound, professional analytic products (intelligence)." One way to accomplish this is to recommend that products meet substantive criteria. The International

Association of Law Enforcement Intelligence Analysts' (IALEIA) *Law Enforcement Analytic Standards* booklet provides standards for analysis that correspond to the intelligence process. These standards focus on:

- Planning
- Direction
- Collection
- Legal constraints
- Evaluation
- Collation
- Analytic accuracy
- Computerized analysis
- Analytic product content
- Analytic outcomes
- Dissemination plan
- Analytic report
- Analytic product format
- Analytic testimony
- Data source attribution
- Analytic feedback
- Analytic production evaluation

It is recommended that analysts or individuals fulfilling the analytic function adhere to the standards outlined in the booklet. A copy of the booklet is included on the resource CD.

## Infrastructure Assessment and Resources

A significant role for any fusion center concerned with homeland security is tracking critical infrastructure and assessing the likelihood of it being the target of a terrorist attack. It is imperative that there is collaboration between center personnel and private sector partners when risk assessments are being conducted regarding the private sector. The private sector has detailed knowledge of its information, processes, and infrastructure, and its subject-matter experts and security personnel can identify accurate and comprehensive risks. Fusion centers may also analyze risks within the jurisdiction, including those risks associated with public safety and private security. Risk assessments, when performed in conjunction with private sector security and subject-matter experts, will aid the center in identifying key infrastructure when threats are present. Fusion centers may also be tasked with cataloging critical infrastructure; developing a methodology to track intelligence relating to threats, exploitable vulnerabilities, and the consequences of loss of those facilities; maintaining and sharing with partners a list of special events that may pose a threat (e.g., high visibility and large crowds); and developing a mechanism to update this information regularly.

Center personnel must utilize the relationships between regulatory government agencies and the private sector when conducting risk assessments; these relationships have already been established and expertise identified. For the nonregulated industry, center personnel should meet with industry officials to identify the critical infrastructure and what is available. These meetings will also lay the foundation for developing trusted relationships with subject-matter experts. The fusion center should be aware that information gathered by regulatory agencies may be protected by regulations and, therefore, not be subject to dissemination.

In addition, the center may develop assessments of the vulnerabilities and security protocols for critical facilities. This may range from simply maintaining the assessments completed by others to actually participating in on-site assessments. Either way, it is important that the center receive risk assessments to aid in threat identification and prevention. The fusion center may consider working with the area Joint Terrorism Task Force (JTTF), Anti-Terrorism Advisory Council (ATAC), Information Sharing and Analysis Center (ISAC), and the U.S. Department of Homeland Security (DHS), including the USP3 portal, as well as other state and local authorities, to design and implement operational resiliency objectives to include protective measures that mitigate vulnerabilities. Included in the resource documents is a section from the Florida Department of Law Enforcement (FDLE) *Terrorism Protection Manual* that covers critical infrastructure assessments. Industry-specific subject-matter experts should be used to aid in infrastructure assessments and the identification of risks associated with the private sector. Subject-matter experts have the knowledge and training to identify and assess critical infrastructure associated with the private industry and are valuable assets for fusion centers. Furthermore, working with subject-matter experts will demonstrate continued collaboration between private industries and fusion centers and will foster trust and the creation of successful partnerships. If fusion centers are tasked with conducting critical infrastructure assessments, every effort should be made to protect the results of these assessments. This information is sensitive and must not be released to nonauthorized personnel. Center management should be aware of local, state, and federal laws regarding the storing and release of this information.

The DHS Office of Preparedness and Office of Intelligence and Analysis (OPOIA) helps deter, prevent, and mitigate consequences in "all-hazard" environments, assessing threats, exploitable vulnerabilities, and consequences. Developed as a result of the Critical Infrastructure Information Act, the OPOIA can aid centers with assessments, risk analysis, and compilations of critical infrastructure assets. More information regarding these programs can be viewed at [www.dhs.gov](http://www.dhs.gov).

## Available Resources on Fusion Center CD

- DHS's *National Response Plan*, December 2004
- *Terrorism Protection Manual*, FDLE, February 28, 2003