

# Guideline 1

Adhere to the *National Criminal Intelligence Sharing Plan* (NCISP) and other sector-specific information sharing plans, and perform all steps of the intelligence and fusion processes.

## The NCISP and the Intelligence and Fusion Processes

### Justification

After the tragic events of September 11, 2001, law enforcement executives and intelligence experts nationwide agreed that law enforcement agencies must work together to develop the capability to gather information, produce intelligence, and share that intelligence with other law enforcement and public safety agencies. The *National Criminal Intelligence Sharing Plan* (NCISP or Plan) was developed in response to this need.

The NCISP provides model standards and policies, recommends methodologies for sharing classified reports, and recommends a nationwide sensitive but unclassified (SBU) communications capability for criminal intelligence sharing. The Plan is a living document that provides local, state, tribal, and federal law enforcement agencies the tools and resources necessary for developing, gathering, accessing, receiving, and sharing intelligence. It is the blueprint that law enforcement agencies can employ to support their crime-fighting and public safety efforts while leveraging existing systems and networks. The Plan is not a system or a network, nor is it technology-based. It is the framework for the development and sharing of intelligence. It supports collaboration and fosters an environment in which all levels of law enforcement work together to improve the safety of our nation.

The NCISP is founded on the concept of intelligence-led policing and encourages law enforcement agencies to embrace and integrate intelligence-led policing elements in their efforts. Proactive instead of reactive, intelligence-led policing allows law enforcement to:<sup>24</sup>

- Describe, understand, and map criminality and the criminal business process.
- Make informed choices and decisions.
- Engage the most appropriate tactics.

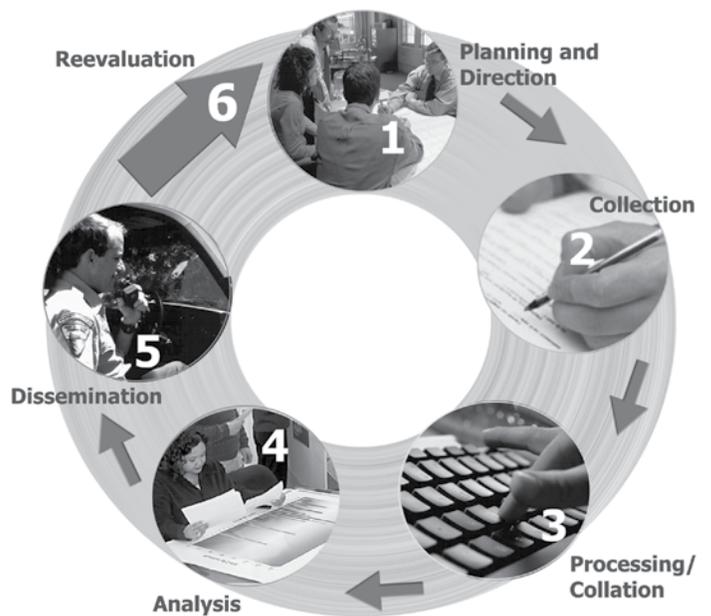
<sup>24</sup> Ronald Bain, "The Dynamics of Retooling and Staffing: Excellence and Innovation in Police Management," Canadian Police College, 2003.

- Target resources.
- Disrupt prolific criminals.
- Articulate a case to the public and in court.

Intelligence-led policing also provides advantages to public safety and private sector components, including trends in criminal activity and increased information sharing with law enforcement to address crime prevention efforts.

Criminal intelligence is the result of a process involving planning and direction, information collection, processing/collation, analysis, dissemination, and reevaluation of information on suspected criminals and/or organizations. This sequential process is commonly referred to as the intelligence process (or cycle). There are various models of the intelligence process in use; however, most models contain the basic steps depicted in the following graphic:

### The Intelligence Process



# Intelligence Process

The intelligence process is the means of developing raw information into finished intelligence products for use in decision making and formulating policies/actions. The first step, planning and direction, involves identifying the need for data. Agency members should engage in a process of deciding what they want to know (or what they need to collect) before they collect it, or they may obtain indiscriminate, unfocused information.

Collection is the gathering of the raw data needed to produce intelligence products. Data may be collected from many sources, including but not limited to public records, the Internet, confidential sources, incident reports, and periodicals.

The next step, processing and collation, involves evaluating the information's validity and reliability. Collation entails sorting, combining, categorizing, and arranging the data collected so relationships can be determined.

Analysis transforms the raw data into products that are useful. This is also the function that separates "information" from "intelligence." It is this vital function that makes the collection effort beneficial. Without this portion of the process, we are left with disjointed pieces of information to which no meaning has been attached. The goal is to develop a report that connects information in a logical and meaningful manner to produce



an intelligence report that contains valid judgments based on analyzed information.<sup>25</sup>

Dissemination is also vital. Without disseminating the intelligence developed, it is pointless to collect it. To be useful, the intelligence disseminated must be timely and credible. Dissemination must also be evaluated based on a right to know and the need to know. The right to know means the recipient has the legal authority to obtain the information pursuant to court order, statute, or decisional law. The need to know means the requestor has the need to obtain information to execute official responsibilities.<sup>26</sup> When dissemination occurs, it is imperative to include all components of fusion centers, including the public safety and private sectors.

The final step involves evaluation/reevaluation of the process performed and the products produced. Evaluation/reevaluation assesses current and new information, assists in developing an awareness of possible weak areas as well as potential threats, and strives to eliminate previously identified weaknesses that have been hardened as a result of the fusion process. Overall, this step provides an opportunity to review the performance or effectiveness of the fusion center's intelligence function.<sup>27</sup>

As previously indicated, fusion centers have improved law enforcement's ability to fight crime and terrorism. Ensuring that each step within the process is followed will facilitate the production of useful intelligence. Nontraditional collectors of information, e.g., the private sector, fire, public works, and public health, are vital to successfully complete the intelligence process. While law enforcement has intelligence information and expertise, the public safety and private sectors have the information systems, processes, and infrastructure that may be targets of crime and terrorism. Further, fusion, through managing the flow of information and intelligence across all levels and sectors of government, integrates the intelligence process to accomplish this sharing. The intelligence process provides a framework for the fused information to be turned into intelligence. Fusion centers utilize the intelligence process to analyze threat-related intelligence and information. These centers are not simply information collection hubs but venues to bring together appropriate partners to prevent crime- and terrorism-related incidents.

## The Fusion Process

The stages of the fusion process generally correlate with the intelligence cycle. The Homeland Security Advisory Council's (HSAC) *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report details the stages of fusion and how to implement the process.<sup>28</sup> The first stage, the management and governance stage, establishes the foundation for fusion in that it overviews the need for a

<sup>25</sup> Bob Morehouse, "The Role of Criminal Intelligence in Law Enforcement." Marilyn B. Peterson (Managing Ed.), Bob Morehouse, and Richard Wright (Eds.), *Intelligence 2000: Revising the Basic Elements*, Sacramento, CA: Law Enforcement Intelligence Unit and Lawrenceville, NJ: International Association of Law Enforcement Intelligence Analysts, Inc., 2000, pp. 1-12.

<sup>26</sup> *Ibid*, p. 9.

<sup>27</sup> *The National Criminal Intelligence Sharing Plan*, 2003, p. 7.

<sup>28</sup> This report, including a comprehensive explanation of the fusion process, can be found in its entirety in Appendix D.

management structure, who the stakeholders are, and fusion center goals and objectives.

The second stage, planning and requirements development, lays the foundation for the types of information that will be collected. This phase establishes where information will come from and the types of information the fusion center will collect. It also provides collection limitations and privacy issues that affect collection and sharing of information.

Collection is the third stage of the process during which the planning and requirements development stage becomes operational. This is when information is collected from various sources, including law enforcement agencies, public safety agencies (e.g., health, fire, and transportation), and the private sector. This stage is essential for fusion centers to be effective.

The fourth stage, analysis, is similar to the analysis phase in the intelligence cycle in that it is during this stage that the information collected is turned into actionable intelligence. One of the goals of the fusion center during this stage is to identify trends or information that will prevent a terrorist attack or other criminal activity.

The fifth stage is dissemination, tasking, and archiving. During this stage, the information that has been collected and analyzed is then disseminated to stakeholders.

The sixth stage is reevaluation. The purpose of this stage is for the fusion center and stakeholders to ensure that what is being collected, analyzed, and disseminated is factual, timely, and relevant. It is during this stage that tweaks and improvements are made to the fusion process.

The last stage is the modification of the requirements stage (Stage 2). After reevaluation occurs and improvements or changes are identified, this stage allows the improvements to be implemented and the process refined.<sup>29</sup>

Often, gaps in the intelligence process exist. To assist in closing these gaps, the Federal Bureau of Investigation (FBI) developed a template to assist agencies in identifying and tracking intelligence gaps. A summary of the FBI's Intelligence Requirements and a copy of the template can be found in *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* (Carter, November 2004).<sup>30</sup> A copy of this guide is included on the resource CD. It is recommended that fusion centers create a formal intelligence and information requirements process that prioritizes and guides the intelligence function.

<sup>29</sup> *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report.

<sup>30</sup> Available on the Community Oriented Policing Services (COPS) Web site at [www.cops.usdoj.gov/Default.asp?Item=1404](http://www.cops.usdoj.gov/Default.asp?Item=1404).

## Issues for Consideration

When implementing portions of the NCISP, consider these steps to help establish or enhance an intelligence component of a fusion center:

- Recognize your responsibilities and lead by example.
- Establish a mission statement and a policy to address developing and sharing intelligence data within your agency.
- Connect to your state criminal justice network and regional intelligence databases, and participate in information sharing initiatives.
- Ensure privacy is protected in policy and practice.
- Access law enforcement Web sites, subscribe to law enforcement listservs, and use the Internet as an information resource.<sup>31</sup>
- Provide your agency members with appropriate training on the criminal intelligence process.
- Become a member in your Regional Information Sharing Systems (RISS) center.
- Become a member of the FBI's Law Enforcement Online (LEO).
- Partner with public and private infrastructure owners and operators.
- Participate in local, state, and national intelligence organizations.
- Participate in the U.S. Department of Homeland Security's (DHS) Homeland Security Information Network (HSIN) Program.
- Ensure the fusion center is fully utilizing the jurisdiction's existing networks and information repositories for criminal and hazard information.

## Available Resources on Fusion Center CD

- [10 Simple Steps to help your agency become a part of the National Criminal Intelligence Sharing Plan](#)
- HSAC's *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion* report
- *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement*
- Law Enforcement Intelligence Unit (LEIU) Audit Checklist
- *National Criminal Intelligence Sharing Plan* report

<sup>31</sup> Prior to entering the public Internet as a law enforcement officer or intelligence organization, consult with jurisdiction and department legal advisors to ensure compliance with any policy or regulation concerning law enforcement intelligence use of the Internet for information sharing. Furthermore, using the official government identity and information system for Internet searching can pose a security risk to the agency network and subject of the search. Explore different ways to avoid such risks with competent technical and legal authorities.