National Criminal Intelligence Sharing Plan

Building a National Capability for Effective Criminal Intelligence Development and the Nationwide Sharing of Intelligence and Information:

The next step in the evolution of the National Criminal Intelligence Sharing Plan

Version 2.0

October 2013

Bureau of Justice Assistance
U.S. Department of Justice

Version 2.0

National Criminal Intelligence Sharing Plan

Building a National Capability for Effective Criminal Intelligence Development and the Nationwide Sharing of Intelligence and Information:

The next step in the evolution of the National Criminal Intelligence Sharing Plan

October 2013

Table of Contents

v Executive Summary

1 Why Should My Agency Have an Intelligence Capability?

4 Background and Purpose

7 Framework for Criminal Intelligence Development and the Nationwide Sharing of Intelligence and Information

14 Implementing the Critical Elements: Recommendations

- 15 Leadership
- 17 Partnerships
- 20 Privacy, Civil Rights, and Civil Liberties (P/CRCL) Protections
- 22 Policies, Plans, and Procedures
- 23 Intelligence Process
- 29 Training
- 30 Security and Safeguarding
- 32 Technology and Standards
- 36 Sustainability

37 Appendix A—Endnotes

38 Appendix B—Resources

40 Appendix C—Accomplishments

44 Appendix D—CICC Membership

45 Appendix E—Glossary

49 Appendix F—Acronyms

About the Criminal Intelligence Coordinating Council

The Criminal Intelligence Coordinating Council (CICC), on behalf of the Global Justice Information Sharing Initiative (Global), developed this resource to support justice agencies in their efforts to implement an intelligence capability within their agency and share information and intelligence nationwide. The CICC, established in May 2004, provides recommendations in connection with the implementation and refinement of the *National Criminal Intelligence Sharing Plan* (NCISP). The CICC is made up of members representing law enforcement and homeland security agencies from all levels of government and is an advocate for state, local, and tribal law enforcement and their efforts to develop and share criminal intelligence for the purpose of promoting public safety and securing the nation. For more information on the CICC, please refer to: www.it.ojp.gov/cicc.

Executive Summary

September 11, 2001, was a watershed moment for American law enforcement; after the widespread and coordinated terrorist attacks, law enforcement leadership acknowledged the criticality of enhancing and improving the development and sharing of criminal intelligence to prevent a terrorist attack from happening again. Numerous improvements and advancements have been realized since 9/11, but the threat remains, as evidenced by plots against the New York Stock Exchange, an attempted car bombing in Times Square, an alleged suicide bombing plot against the United States Capitol, and the Boston Marathon bombings.

One of the most notable actions that resulted from September 11 was the development and release of the 2003 ***National Criminal Intelligence Sharing Plan*** (NCISP). The 2003 NCISP was designed by state, local, tribal, and federal law enforcement partners to provide a path forward in improving the collection and analysis of information to create valuable and actionable intelligence products. Further, the NCISP highlighted that the sharing of intelligence products among state, local, tribal, and federal partners is critical in the prevention of terrorism and other criminal activity.

NCISP, Version 1: Released in 2003, it identifies solutions and approaches to improve the nation's ability to develop and share criminal intelligence.

NCISP, Version 2: Released in 2013, it identifies additional recommendations and action items regarding the development and sharing of criminal intelligence and the sharing of information.

The NCISP marked a transformation in American law enforcement, notably that every agency, regardless of size, has a stake in the development and sharing of criminal intelligence. From a small ten-person police department to a large state investigative agency, all law enforcement can and should be a part of the intelligence process, thereby improving the safety of the nation and its citizens.

Over the last ten years, the NCISP has assisted law enforcement agencies across the United States in making modifications and enhancements to their internal business processes to facilitate the availability, accessibility, and flow of criminal intelligence. The results of this widespread implementation have been improvements in the collection of information, the analysis of this information, and the sharing of criminal intelligence. However, with an evolving crime outlook both in the homeland and internationally, it is imperative to review long-standing recommendations to identify new opportunities and approaches that promote continued nationwide criminal intelligence sharing. Thus, in 2013 the decade-old NCISP was reviewed and enhanced, resulting in the release of version 2.0.

Version 2.0 of the NCISP is designed to build on the recommendations identified ten years ago and to further promote responsible and effective criminal intelligence and information sharing. This "refresh" expands the original focus to include recommendations that address the sharing of criminal intelligence and information externally (or outside a law enforcement agency) with other state, local, tribal, and federal law enforcement agencies and/or homeland security partners.

The NCISP is founded on the notion that an intelligence capability is imperative to agency operations. An intelligence capability supports agency executives as they enhance police operations through

recommendations on resource allocation, identification of crime "hot spots" in a jurisdiction, and analysis of emerging criminal activity within a region. Every agency should develop and maintain an intelligence capability that is suitable for its size and available resources, and version 2.0 of the NCISP provides recommendations and action items for agency leadership to continue to build and enhance intelligence-related operations. A foundational element of version 2.0 of the NCISP is that it is designed to support all agencies, regardless of size or resources, as they establish an agency intelligence capability at some level, thereby facilitating widespread development and sharing of criminal intelligence and the widespread sharing of information.

To assist agencies in developing this capability and sharing on a nationwide level, the NCISP identifies nine critical elements and multiple recommendations and action items. These critical elements, recommendations, and action items illustrate the suggested way forward for the achievement of an optimized means of developing and sharing criminal intelligence and sharing information.

1. Leadership—The driving force of every agency or organization is its leadership. The NCISP recognizes this element of organizational culture and focuses this section on law enforcement executives and organizational leadership in the critical role they play in their recognition of the NCISP (and its tenets), as well as their commitment to support its implementation. Advocacy, support, commitment, and outreach are a few of the topics covered in this section.
2. Partnerships—Partnership development supports agency missions and functionality. In an era of changing crime, partnerships can assist in the identification, mitigation, and investigation of crime and can improve community relations. This section focuses on the importance of building partnerships with both law enforcement and non-law enforcement agencies and entities and the value of these partnerships to the safety of communities.
3. Privacy, Civil Rights, and Civil Liberties Protections—One of the primary concerns of law enforcement agencies across the nation is the protection of the privacy, civil rights, and civil liberties (P/CRCL) of those they serve. This section emphasizes the importance of protecting P/CRCL in the implementation of the NCISP and the effective development and sharing of criminal intelligence and information. The development of guidance documents and templates to assist with further protections of these rights and liberties is also addressed in this section.
4. Policies, Plans, and Procedures—It is imperative that agencies and organizations have policies, plans, and procedures in place to ensure effective and efficient operations and at the same time protect agencies and organizations from undue harm and reduce risk. This section details how agencies can address internal operations to help ensure a level of consistency among policies, plans, and procedures nationwide. Common policies, plans, and procedures will facilitate improved and enhanced development and sharing of criminal intelligence and information. 28 Code of Federal Regulations Part 23 (28 CFR Part 23) and various nationally recognized model policies are highlighted in this section.

5. Intelligence Process—Every law enforcement agency should have an intelligence capability. Agencies that participate in the intelligence process, regardless of their level of participation, stand to gain considerable value and significantly improve their crime-reduction efforts. Participation may be as basic as the simple collection and sharing of information with a nearby fusion center or task force, combined with the receipt of future intelligence products from that entity that can be shared with appropriate agency personnel. This element encourages participation in the intelligence process as well as the enhancement of agency intelligence functions, regardless of agency size or resources, by providing scalable recommendations that are achievable by agencies with various capacities and budgets. Leveraging information and analysis to direct policing efforts—or intelligence-led policing—is highlighted, along with the applicability of coordinating with various investigative task forces, intelligence centers, and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). Recommendations also address analysts and agency information needs.

6. Training—As their environment changes, law enforcement and homeland security officials must meet new challenges head-on. Meeting these challenges requires training, which helps ensure the safety of both the officers in the field and those they serve while maintaining effective policing strategies and fulfilling the agency mission. This section discusses training components and the avenues needed (such as distance-learning platforms) to implement the tenets of the NCISP.

7. Security and Safeguarding—Law enforcement and homeland security agencies have significant technological investments to support their mission to protect the communities they serve. These investments include information management and data communications technologies to better enable the agency mission. With the increase in technology comes new vulnerabilities. As such, the implementation of stringent security measures, operational and technological, utilizing national standards and best practices is imperative. This section elaborates on the security initiatives and resources available to law enforcement and homeland security agencies to assist them in the adoption and use of information sharing and safeguarding standards to protect their information sharing environments from cyberattack and also offers guidance in the area of security clearances.

8. Technology and Standards—Technology is ever-changing, which presents both opportunities and obstacles for law enforcement agencies as they build their criminal intelligence capacities. As expressed in the President's *National Strategy for Information Sharing and Safeguarding*, "There is no greater responsibility than ensuring the safety and security of the United States and the American people [which] . . . demands the timely and effective sharing of intelligence and information about threats to our Nation with those who need it, from the President to the police officer on the street." Standards-based technological approaches will help minimize obstacles and extend the lifelines of some technology products (such as legacy systems). This section addresses the use of technological advancements and application of standards to support achievement of the NCISP's recommendations, which include simplifying the access to and sharing of information across various systems.

9. Sustainability—Sustainability plans are critical to the longevity of any initiative. These plans ensure that the lifeblood and resources of an initiative remain healthy enough for operations to continue. These plans may come in all shapes and sizes and will vary greatly depending upon such factors as mission, type of service, and level of service delivered. This section focuses on the need for sustainability planning to help ensure longevity for the participants in the NCISP's Framework as well as the NCISP itself.

It is the ultimate goal of the NCISP to continue to support law enforcement agencies and leadership in the identification of solutions and approaches for a cohesive plan to improve the nation's ability to develop and share criminal intelligence. The NCISP aims to bring together state, local, tribal, and federal law enforcement agencies and partners, preparing the nation as it continues to fight all crimes and terrorism to keep communities safe.

"Every law enforcement agency can have an intelligence capability, regardless of agency size."

—Sheriff Mark Wasylyshyn, Wood County, Ohio, Sheriff's Office

Why Should My Agency Have an Intelligence Capability?

A frequent question asked by many state, local, and tribal law enforcement officials is "Why should my agency have an intelligence capability?" Law enforcement agencies have a multitude of public safety responsibilities and may question whether implementing an intelligence capability would stretch agency resources too far. However, as individuals in agency leadership pursue more cost-effective measures and aim to "maximize resources" to the fullest extent possible, an intelligence capability may assist them in more efficiently allocating resources, enhancing crime prevention tactics, and expediting both investigating and solving criminal activity. Consider the potential benefit of 800,000 law enforcement officers contributing to the intelligence process and sharing information. The impact of that collective force would be paralyzing on crime, while providing an exponential increase to community safety nationwide.

An intelligence capability is defined as "an agency's ability to perform an act or acts included in the intelligence process or cycle."

An *intelligence*[1] *capability* is defined as "an agency's ability to perform an act or acts included in the intelligence process or cycle."[2] An intelligence capability is achievable by any agency . . . *regardless of size*! This ability can range from assigning a single point of contact in the agency to gather tips, leads, and suspicious activity reports (SARs) to share with a fusion center, to a small unit of two to three officers and analysts who analyze information and intelligence data in order to identify emerging crime trends, to a comprehensive intelligence unit of ten or more law enforcement personnel who develop criminal intelligence, situational awareness bulletins, and intelligence reports for line officers to assist in their public safety responsibilities. Implementing an intelligence capability, no matter how big or small, can have a significant impact on all crimes and terrorism.

Example

A young child was reported missing from an apartment complex in northern Georgia. After the Georgia Bureau of Investigation (GBI) identified a suspect in the case, the GBI analysts assigned to the Georgia Information Sharing and Analysis Center (GISAC), the state fusion center, began developing information on the suspect. Upon determining that the subject had previously lived in Virginia, the GISAC contacted the Virginia Fusion Center (VFC) and requested an urgent records check on the subject. The VFC searched the various Virginia databases and was able to find information in one of their systems regarding previous contacts with law enforcement. The VFC immediately responded to Georgia with an update that the suspect had previously been the subject of a local police report. Based on this information, the GISAC was able to request the full report from local Virginia authorities, and GBI Special Agents were sent to Virginia to reinterview the complainant documented in the report. The information obtained from the VFC and local Virginia authorities was essential to the investigation. Shortly thereafter, the subject was arrested and charged with the murder of the child.

The example above demonstrates the value and relevancy of an intelligence capability. An intelligence capability offers an agency or an organization the opportunity to be proactive in its mission, be it through crime prevention efforts or the thwarting of a potential terrorism event. An important aspect of an intelligence capability is information sharing, both internally and externally. The sharing of criminal information and intelligence has far-reaching benefits for the communities that law enforcement and homeland security organizations serve, and an intelligence capability can be used as the agency's focal point in this sharing priority.

The implementation of an intelligence capability is scalable. Every law enforcement agency, regardless of the number of personnel or the size of the jurisdiction, has an important role in the development and sharing of criminal intelligence and information to protect its communities. From designating an officer who regularly interacts with a task force to creating an internal intelligence unit that provides a full-time representative to a fusion center, there are many opportunities for agencies to establish an intelligence capability within their organization.

An intelligence capability should not be viewed as burdensome or cost-prohibitive for an agency. An intelligence capability enables an agency to gather, share, and receive criminal intelligence and information. This capability may include the reporting of suspicious activity by a frontline officer or the distribution of a bulletin produced by a fusion center to all agency personnel. If every agency has an intelligence capability, greater information sharing can occur locally, regionally, and nationally, which will improve the intelligence development process for the nation as a whole, thereby improving prevention, mitigation, and investigative efforts.

The development and implementation of an intelligence capability, regardless of the size of the agency, begins the same way—with a plan.

The concept of "policing with a plan" is as simple as drafting a policy that states how the agency will gather information and intelligence and what the agency will do with this information and intelligence to further the agency mission. This plan will vary between agencies, but every plan has the same goal: incorporating the development and sharing of criminal intelligence and information to protect communities.

Version 2.0 of the *National Criminal Intelligence Sharing Plan* (NCISP) was developed to illustrate the value of criminal intelligence and information sharing to agency leadership and communicate how to develop a plan to establish a realistic, achievable intelligence capability. Version 2.0 of the NCISP identifies critical elements (Leadership, Partnerships, Training, etc.), that are used to organize the recommendations contained in version 2.0 and also serve as chapters or sections within the document. By organizing the recommendations in this manner, agency executives will be able to prioritize the implementation of the NCISP's recommendations, section by section, according to their agencies' specific needs and resources. All agencies—from a 15-person police department to a 1,500-person sheriff's office—should strive to implement an intelligence capability that is suitable for their agency's capacity and will support the safety and security of their communities and, collectively, the nation.

Getting Started—Examples of What Agencies Can Do With Minimal Investment

Examples

- Suspicious Activity Reporting (SAR) Line Officer Training:
  nsi.ncirc.gov/training_sarlot.aspx
- 28 Code of Federal Regulations Part 23 (28 CFR Part 23) Training:
  ncirc.gov/28cfr/default.aspx
- Regional Information Sharing Systems® (RISS):
  Contact RISS or your nearest High Intensity Drug Trafficking Area (HIDTA) point of contact to set up a deconfliction system.
- Fusion Centers:
  A listing of state and major urban fusion centers is available at
  dhs.gov/contact-fusion-centers

Background and Purpose

From the 1950s to the 2000s, law enforcement agencies addressed crime and its evolution with improved strategies and began to share critical information with each other. However, it was the events of 9/11 that served as a catalyst for state, local, tribal, territorial, and federal law enforcement and homeland security agencies to improve their ability to develop and share criminal intelligence and information. This need culminated in the 2003 release of the *National Criminal Intelligence Sharing Plan* (NCISP), which provides the blueprint to help agencies establish criminal intelligence sharing policies, procedures, standards, technologies, and training. The NCISP was groundbreaking in that it brought together representatives from national law enforcement and homeland security associations and organizations with the goal of working together to establish a collective path forward to strive to prevent another 9/11-type event. The tenets and principles identified in the 2003 NCISP are reflected in numerous national initiatives that have been established and implemented since 2003, including:

- The Criminal Intelligence Coordinating Council: The creation of the Criminal Intelligence Coordinating Council (CICC) was called for in the NCISP to provide guidance consistent with its recommendations. What has resulted is a body that advocates for state, local, and tribal law enforcement agencies and personnel and supports their efforts to develop and share criminal intelligence and information for the purpose of promoting public safety and securing the nation.
- The National Network of Fusion Centers: State and major urban area fusion centers (fusion centers) serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of major crime and threat-related information between the federal government and state, local, tribal, territorial (SLTT), and private sector partners.[3] Fusion centers operate off of an established set of guidelines (*Fusion Center Guidelines*, https://it.ojp.gov/gist/94/) and capabilities (*Baseline Capabilities for State and Major Urban Area Fusion Centers*, https://it.ojp.gov/gist/39/) that recognize and account for the fact that

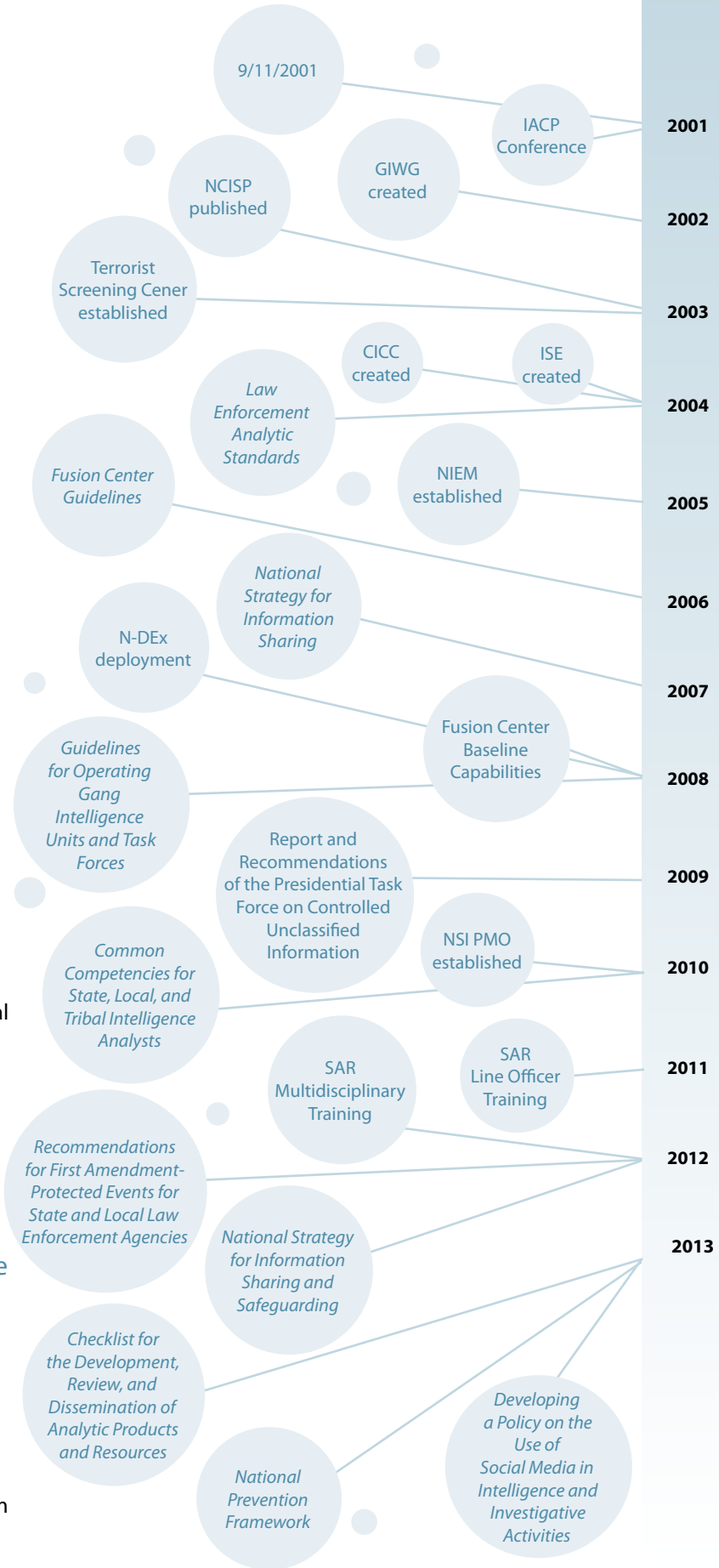
the missions of fusion centers vary based on the environment in which the center operates, be it an "all-crimes" or an "all-hazards" approach. The strategies and the U.S. Department of Homeland Security (DHS) support and encourage these approaches, while respecting that a fusion center's mission should be defined based on jurisdictional needs.

> *National Strategy for Information Sharing and Safeguarding* (NSISS): National security depends on our ability to share the right information with the right people at the right time. Anchored on the 2010 National Security Strategy, the *National Strategy for Information Sharing and Safeguarding* (NSISS) (http://www.whitehouse.gov/the-press-office/2012/12/19/national-strategy-information-sharing-and-safeguarding) provides guidance for more effective integration and implementation of policies, processes, standards, and technologies that promote secure and responsible national security information sharing. This Strategy does not replace the *National Strategy for Information Sharing* (2007 NSIS) (http://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf), as the 2007 NSIS continues to provide a policy framework and directs many core initiatives intended to improve information sharing.

> Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): The NSI provides law enforcement with tools to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. The NSI is a standardized process for identifying and reporting suspicious activity in jurisdictions across the country and also serves as the unified focal point for sharing SAR information.[4]

> The Law Enforcement National Data Exchange (N-DEx): N-DEx is a repository of criminal justice records, available in a secure online environment, managed by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division. N-DEx uses criminal justice data from state, local, tribal, and federal agencies across the nation to quickly "connect the dots" between data that may seem unrelated.

Notable Accomplishments Since 2001



Version 2.0 of the *National Criminal Intelligence Sharing Plan* (NCISP) builds upon the tenets and recommendations from the 2003 version through the identification of a new set of recommendations, all focused on the continued assistance to state, local, tribal, territorial, and federal law enforcement and homeland security agencies and organizations in developing and enhancing an intelligence capability that can be integrated into nationwide criminal intelligence and information sharing efforts.

In addition to demonstrating how the concepts of the NCISP have been implemented over the last ten years, particularly the improved and enhanced partnerships that have developed at all levels of government, these initiatives demonstrate the need for the CICC to update the 2003 version to reflect the current information sharing landscape and also identify the gaps and the need for guidance in the next ten years. The need to "refresh" the 2003 NCISP was initially discussed by the CICC in 2011, as a part of the 10-year anniversary of 9/11 and an assessment of the current criminal intelligence sharing environment. As a result of this discussion, the CICC established a task team charged with reviewing the 28 original recommendations of the 2003 version and identifying new recommendations to further the core mission of the NCISP in addressing all crimes and terrorism.

This task team, mirroring the development process of the 2003 version, was made up of members of the national law enforcement and homeland security associations, including the International Association of Chiefs of Police, the National Sheriffs' Association, the Major Cities Chiefs Association, the Major County Sheriffs' Association, the Association of State Criminal Investigative Agencies, and the National Fusion Center Association, as well as federal partners from the FBI, the U.S. Department of Homeland Security (DHS), the U.S. Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the Office of the Director of National Intelligence (ODNI). The task team studied the recommendations of the 2003 NCISP, discussed how (and whether) the recommendations have been implemented, validated the recommendations (as appropriate), and identified new recommendations and action items to continue to improve, enhance, and expand the nation's ability to develop and share criminal intelligence and information.

What has resulted is the 2013 release of version 2.0 of the NCISP. This version builds upon the tenets and recommendations from the 2003 version through the identification of a new set of recommendations, all focused on the continued assistance to state, local, tribal, territorial, and federal law enforcement and homeland security agencies and organizations in developing and enhancing an intelligence capability that can be integrated into nationwide criminal intelligence and information sharing efforts.

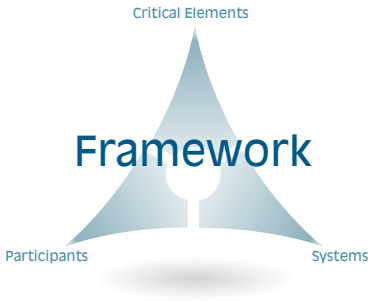
It is important to note that the 2003 version of the NCISP is still relevant, and agencies should continue to strive to implement the tenets of the original NCISP. The 2003 version was designed to provide guidance to agencies with recommendations to develop and incorporate an intelligence process into their operations, establish standards, and enhance information sharing systems and security while maintaining stringent protections on individuals' privacy, civil rights, and civil liberties and still has relevance in today's information sharing landscape. Version 2.0 of the NCISP broadens this original focus (to include all crimes), expanding beyond internal agency operations, and aims to support the establishment of a nationwide framework linking individual agencies' intelligence capabilities on a national scale while maintaining an unwavering dedication to the protection of privacy, civil rights, and civil liberties.

Framework
for Criminal Intelligence Development and the Nationwide Sharing of Intelligence and Information

Effective criminal intelligence development and the nationwide sharing of intelligence and information are contingent on a defined framework to ensure that all law enforcement and homeland security components (state, local, tribal, and federal partners) share a common understanding with respect to what is being shared, how to share it, and what protections need to be in place. The NCISP lays the foundation for this Framework through:

- The identification of *nine critical elements* that encompass the most critical aspects of effective criminal intelligence development and the sharing of intelligence and information.
- The *participants* (state, local, tribal, and federal government and the private sector) that implement these critical elements.
- The *systems* that provide the infrastructure and are used in criminal intelligence development and the sharing of intelligence and information.

The illustration below depicts the integration of the three components (critical elements, information sharing participants, and systems) that are reliant on one another and key to the success of the Framework.



The Framework acknowledges the *Domestic Approach to National Intelligence*, as well as the U.S. Intelligence Community (IC) (which maintains a focus on foreign intelligence and national security initiatives), its components, and its connection to the Framework and thereby its connection to state, local, and tribal law enforcement and homeland security agencies. The Framework also acknowledges that the sharing of information and intelligence supports our national preparedness efforts beyond terrorism, as outlined in Presidential Policy Directive 8: National Preparedness and the National Prevention Framework. This guidance encourages the sharing of information—whether it be terrorism-related, criminal in nature, or pertaining to other hazards or incidents. Such efforts include coordination of and collaboration between investigative, analytical, and intelligence entities such as fusion centers, Joint Terrorism Task Forces (JTTFs), High Intensity Drug Trafficking Area (HiDTA) Programs, and Regional Information Sharing Systems® (RISS) Centers, as well as the effective sharing of information to support and inform operational response efforts, such as those activities managed by Emergency Operations Centers (EOCs).

Nine Critical Elements

1. Leadership
2. Partnerships
3. Privacy, Civil Rights, and Civil Liberties Protections
4. Policies, Plans, and Procedures
5. Intelligence Process
6. Training
7. Security and Safeguarding
8. Technology and Standards
9. Sustainability

Critical Elements

Nine critical elements have been strategically identified to facilitate a national capability to develop criminal intelligence and share criminal intelligence and information. These critical elements help organize the collection of recommendations contained in version 2.0 and serve as chapters or sections within the document. This format will assist agency executives in prioritizing the implementation of the NCISP's recommendations according to their agencies' specific needs and resources. The nine critical elements and their respective recommendations and action items strategically support each other. Agencies should strive to implement all of the recommendations contained in the NCISP as resources allow.

1. Leadership—The driving force of every agency or organization is its leadership. The NCISP recognizes this element of organizational culture and focuses this section on law enforcement executives and organizational leadership in the critical role they play in their recognition of the NCISP (and its tenets), as well as their commitment to support its implementation. Advocacy, support, commitment, and outreach are a few of the topics covered in this section.
2. Partnerships—Partnership development supports agency missions and functionality. In an era of changing crime, partnerships can assist in the identification, mitigation, and investigation of crime and can improve community relations. This section focuses on the importance of building partnerships with both law enforcement and non-law enforcement agencies and entities and the value of these partnerships to the safety of communities.
3. Privacy, Civil Rights, and Civil Liberties Protections—One of the primary concerns of law enforcement agencies across the nation is the protection of the privacy, civil rights, and civil liberties (P/CRCL) of those they serve. This section emphasizes the importance of protecting P/CRCL in the implementation of the NCISP and the effective development and sharing of criminal intelligence and information. The development of guidance documents and templates to assist with further protections of these rights and liberties is also addressed in this section.
4. Policies, Plans, and Procedures—It is imperative that agencies and organizations have policies, plans, and procedures in place to ensure effective and efficient operations and at the same time protect agencies and organizations from undue harm and reduce risk. This section details how agencies can address internal operations to help ensure a level of consistency among policies, plans, and procedures nationwide. Common policies, plans, and procedures will facilitate improved and enhanced development and sharing of criminal intelligence and information. 28 Code of Federal Regulations Part 23 (28 CFR Part 23) and various nationally recognized model policies are highlighted in this section.

5. **Intelligence Process**—Every law enforcement agency should have an intelligence capability. Agencies that participate in the intelligence process, regardless of their level of participation, stand to gain considerable value and significantly improve their crime-reduction efforts. Participation may be as basic as the simple collection and sharing of information with a nearby fusion center or task force, combined with the receipt of future intelligence products from that entity that can be shared with appropriate agency personnel. This element encourages participation in the intelligence process as well as the enhancement of agency intelligence functions, regardless of agency size or resources, by providing scalable recommendations that are achievable by agencies with various capacities and budgets. Leveraging information and analysis to direct policing efforts—or intelligence-led policing—is highlighted, along with the applicability of coordinating with various investigative task forces, intelligence centers, and the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). Recommendations also address analysts and agency information needs.

6. **Training**—As their environment changes, law enforcement and homeland security officials must meet new challenges head-on. Meeting these challenges requires training, which helps ensure the safety of both the officers in the field and those they serve while maintaining effective policing strategies and fulfilling the agency mission. This section discusses training components and the avenues needed (such as distance-learning platforms) to implement the tenets of the NCISP.

7. **Security and Safeguarding**—Law enforcement and homeland security agencies have significant technological investments to support their mission to protect the communities they serve. These investments include information management and data communications technologies to better enable the agency mission. With the increase in technology comes new vulnerabilities. As such, the implementation of stringent security measures, operational and technological, utilizing national standards and best practices is imperative. This section elaborates on the security initiatives and resources available to law enforcement and homeland security agencies to assist them in the adoption and use of information sharing and safeguarding standards to protect their information sharing environments from cyberattack and also offers guidance in the area of security clearances.

8. **Technology and Standards**—Technology is ever-changing, which presents both opportunities and obstacles for law enforcement agencies as they build their criminal intelligence capacities. As expressed in the President's *National Strategy for Information Sharing and Safeguarding*, "There is no greater responsibility than ensuring the safety and security of the United States and the American people [which] . . . demands the timely and effective sharing of intelligence and information about threats to our Nation with those who need it, from the President to the police officer on the street." Standards-based

Agencies may prioritize the implementation of these elements and the associated recommendations differently according to their capacity and available resources.

"Incorporation of intelligence development and sharing significantly enhances efficiency in law enforcement operations."

—Sheriff Doug Gillespie, Las Vegas Metropolitan Police Department

technological approaches will help minimize obstacles and extend the lifelines of some technology products (such as legacy systems). This section addresses the use of technological advancements and application of standards to support achievement of the NCISP's recommendations, which include simplifying the access to and sharing of information across various systems.

9. Sustainability—Sustainability plans are critical to the longevity of any initiative. These plans ensure that the lifeblood and resources of an initiative remain healthy enough for operations to continue. These plans may come in all shapes and sizes and will vary greatly depending upon such factors as mission, type of service, and level of service delivered. This section focuses on the need for sustainability planning to help ensure longevity for the participants in the NCISP's Framework as well as the NCISP itself.

Law enforcement and homeland security communities have made great progress in implementing these elements through policy development and guidance, standards development, training programs, and technical assistance. One of the goals of the NCISP is to fuse these elements together to emphasize their value to nationwide criminal intelligence and information sharing.

To assist in full realization of the Framework, the NCISP identifies key tools and resources to effectively help agencies make more efficient use of their current resources while increasing their ability to develop and share criminal intelligence and information on a nationwide scope. The NCISP seeks to minimize requirements for additional agency resources needed to actively participate in this Framework. Law enforcement and homeland security agencies are encouraged to be key mission partners and participate in the NCISP to ensure the success and value of this Framework.

Systems

Though not overtly referenced within the nine critical elements, systems play a critical role in facilitating the development of intelligence and the sharing of both intelligence and information. For this reason, the NCISP identifies systems as one of its foundational elements to fully achieve the Framework.

Key to the success of information sharing systems is both use and interoperability. Agencies across the country have different needs and resources based on the geographic area they cover and the populations they serve. As a result, these agencies may use different systems to meet their specific needs. While these systems may offer different services or applications, at their core, they should all provide basic levels of information management and the ability to share their information with proper agency authorization. Even though information systems may have differences, communication between them can still be achieved through interoperability.

System interoperability is a complex problem. System interoperability is an effective solution for connecting agency systems. However, developing interoperability standards and encouraging law enforcement agencies to utilize systems that meet those standards can be an attainable goal. The NCISP makes recommendations that focus on cooperation and interoperability between systems in order to accommodate all agencies, regardless of size and resources.

Participants

Equally important to the nine critical elements and the systems are the participants that support, implement, and utilize the NCISP and its Framework. This community of users includes:

1. **Criminal justice and state, local, tribal, and territorial law enforcement agencies**—includes local police departments, county sheriffs, state police agencies, tribal police departments, corrections agencies, investigative task forces (both multijurisdictional and multiagency and composed of state and local law enforcement officers), and law enforcement intelligence units.
2. **Federal justice and homeland security agencies**—includes but is not limited to the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), the Office of the Program Manager for the Information Sharing Environment (PM-ISE), the Federal Bureau of Investigation (FBI), the U.S. Drug Enforcement Administration (DEA), and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).
3. **National Network of Fusion Centers**—includes all designated state and major urban area fusions centers, which serve as a focal point for the receipt of information from federal, state, local, tribal, and private sector partners.
4. **Regional Information Sharing Systems (RISS) Centers**—includes the six regional centers across the United States (Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network®, Mid-States Organized Crime Information Center®, New England State Police Information Network®, Rocky Mountain Information Network®, Regional Organized Crime Information Center®, Western States Information Network®).
5. **High Intensity Drug Trafficking Areas (HIDTAs) Program**—includes all of the HIDTAs across the United States and their intelligence programs, operational task forces, and Investigative Support Centers.
6. **Crime analysis centers (CACs)**—Crime analysis centers (CACs) have recently been established in several major cities and urban areas throughout the United States. These high-tech centers utilize a wide range of technological and analytic tools to assist officers during law enforcement situations. CACs are unique in that they provide information and intelligence in real time as officers

Version 2.0 of the *National Criminal Intelligence Sharing Plan* (NCISP) expands its focus to a more enterprise-wide view of intelligence and information sharing, while maintaining an unwavering dedication to the protection of privacy, civil rights, and civil liberties.

All agencies—from a 15-person police department to a 1,500-person sheriff's office—should strive to implement an intelligence capability that is suitable for their agency's capacity and will support the safety and security of their communities and, collectively, the nation.

respond to calls. Many CACs identify crime patterns and criminal-activity hot spots, access multiple data sources, employ sophisticated mapping and video surveillance, monitor ongoing police activities, support situational awareness, and provide critical analytic capabilities.

7. Law enforcement professional organizations—includes but is not limited to the International Association of Chiefs of Police (IACP), the National Sheriffs' Association (NSA), the Major Cities Chiefs Association (MCCA), the Major County Sheriffs' Association (MCSA), the Association of State Criminal Investigative Agencies (ASCIA), the International Association of Law Enforcement Intelligence Analysts (IALEIA), and the National Fusion Center Association (NFCA).
8. Private sector and non-law enforcement organizations—includes private security, fire/emergency medical services (EMS), emergency management, critical infrastructure and key resources (CIKR) partners, and other nongovernmental organizations.

These participants all have a role in criminal intelligence and information development and sharing within the United States. An agreement among the participants to champion the development and sharing of criminal intelligence and information among each other, in accordance with the guidance and recommendations detailed throughout the nine critical elements of the NCISP, completes the cycle and further fortifies communities and the nation.

In addition, these participants, along with the U.S. Intelligence Community (IC), form a complex, federated enterprise. These partners across the enterprise, regardless of their level, play important roles with respect to warning, interdiction, prevention, and response. A *Domestic Approach to National Intelligence* recognizes that the effective integration of criminal intelligence and other information with national intelligence of the IC is essential to protecting our communities, our states, and our nation.

U.S. Intelligence Community

The U.S. Intelligence Community (IC) is a coalition of 17 agencies and organizations within the executive branch that work both independently and collaboratively to gather the intelligence necessary to conduct foreign relations and national security activities. The primary mission of the IC is to collect and convey the essential information the President and members of the policymaking, law enforcement, and military communities require to execute their appointed duties. The following organizations—or elements within them—are members of the IC:

1. Air Force Intelligence
2. Army Intelligence
3. Central Intelligence Agency

4. Coast Guard Intelligence
5. Defense Intelligence Agency
6. Federal Bureau of Investigation
7. Marine Corps Intelligence
8. National Geospatial-Intelligence Agency
9. National Reconnaissance Office
10. National Security Agency
11. Navy Intelligence
12. Office of the Director of National Intelligence
13. U.S. Department of Energy
14. U.S. Department of Homeland Security
15. U.S. Department of State
16. U.S. Department of the Treasury
17. U.S. Drug Enforcement Administration

Members of the IC collect and assess information regarding international terrorist and narcotic activities; other hostile activities by foreign powers, organizations, persons, and their agents; and foreign intelligence activities directed against the United States. As needed, the President may also direct the IC to carry out special activities in order to protect U.S. security interests against foreign threats.

For additional information on the Intelligence Community, please visit the Office of the Director of National Intelligence Web site: http://www.dni.gov/index.html.

"Our nation's public safety community must be prepared for the threats of today and tomorrow by embracing intelligence-led policing and use the NCISP as the blueprint for our homeland and hometown threat mitigation strategy. We must also develop and utilize the analytical capabilities available throughout our regions, states, and nation to more effectively and efficiently deploy our resources to protect the communities we serve. The importance of the NCISP can't be understated, and it must be adopted by every law enforcement agency in the nation and at every level of those organizations."

—Mike Sena
Director, Northern California Regional Intelligence Center

Implementing the Critical Elements: Recommendations

This section identifies recommendations and action items, organized by the nine critical elements, that are crucial to the successful implementation of the NCISP and, more specifically, the nationwide development and sharing of criminal intelligence and information. The recommendations and action items build off the original 28 recommendations published in version 1.0 of the NCISP by:

- Facilitating progress in areas of leadership development, policy development, partnership development, and the intelligence process.
- Providing sustainment to much-needed resources and vital protections (such as privacy, civil rights, and civil liberties).
- Maintaining relevance in areas such as technology and standards, security, and training.

You will also notice various "callout" items strategically placed throughout the critical element sections. These callout items include:

- Resources (which are further expanded upon in Appendix B)
- Success stories
- Tips on getting started
- Clarification points

These items were designed to help you, the reader, more easily understand the intent of the recommendations, see examples of successful real-world applications, and facilitate your agency's involvement in criminal intelligence development and the sharing of intelligence and information.

Leadership

The driving force of every agency or organization is its leadership. The NCISP recognizes this element of organizational culture. This section focuses on law enforcement executives and organizational leadership in the critical role they play in their acceptance of the NCISP and its tenets, as well as their commitment to supporting its implementation. Advocacy, support, commitment, and outreach are a few of the topics covered in this section.

Getting Started

Leadership

> Designate a leader to develop or enhance your agency's intelligence capability.

> Access the Global Information Sharing Toolkit (GIST) (www.it.ojp.gov/gist) for resources to develop and enhance the agency's intelligence capability.

Recommendation: State, local, and tribal law enforcement and homeland security leaders should understand the role of the CICC, which serves as an advocate for law enforcement and homeland security agencies across the nation through its support and coordination in the resolution of policy issues at a national level and should be tasked with supporting the implementation of the tenets of the NCISP.

Action Items

- ✓ The CICC should continue to support the implementation of the NCISP.
- ✓ The CICC should conduct annual reviews of the NCISP and report out on progress in achieving goals and recommendations.

Recommendation: National-level law enforcement and homeland security organizations and associations and other relevant and interested groups should work together to support the NCISP.

Action Items

- ✓ The professional organizations and associations represented on the CICC should consider issuing a resolution to support version 2.0 of the NCISP and continue to implement the recommendations of version 1.0 of the NCISP.
- ✓ National-level organizations and associations should, on an annual basis, develop and/or assess annual action plans associated with the implementation of the tenets of the NCISP by member agencies.

Recommendation: The CICC should develop materials and resources to inform law enforcement agencies and, subsequently, the public of the availability and value of the NCISP and its core concepts. The CICC's membership should disseminate these materials to their agencies and their partners as applicable.

Action Items

- ✓ The CICC should support the development of a dissemination plan to ensure that this overview of version 2.0 of the NCISP is distributed to law enforcement executives across the United States.

Resource Spotlight

Agencies at all levels should consider using the resources developed by state, local, tribal, and federal organizations, through the CICC and the Global Justice Information Sharing Initiative (Global), to demonstrate their commitment to and active implementation of version 2.0 of the NCISP. These resources can be found in the following locations:

- Justice Information Sharing Web site: www.it.ojp.gov/intelligence_products
- National Criminal Intelligence Resource Center (NCIRC): www.ncirc.gov
- Global Information Sharing Toolkit (GIST): www.it.ojp.gov/gist

Success Story
The Smart Policy Initiative

The Smart Policing Initiative (SPI) supports law enforcement agencies in building evidence-based, data-driven law enforcement tactics and strategies that are effective, efficient, and economical. Smart Policing represents a strategic approach that brings more "science" into police operations by leveraging innovative applications of analysis, technology, and evidence-based practices. The goal of the SPI is to improve policing performance and effectiveness while containing costs, an important consideration in today's fiscal environment.

The Bureau of Justice Assistance (BJA) has supported the implementation of SPI projects by 35 police agencies. Working with research partners, these agencies collect and analyze data to devise solutions to problems such as street robberies, juvenile prescription drug abuse, repeat violent offenders, and neighborhood drug markets. The SPI community documents best practices and lessons learned so as to incorporate innovative, economical policing strategies nationwide. As a result of the implementation of SPI and the use of evidence-based research and technical assistance from nationally recognized subject-matter experts, communities across the country have experienced double-digit reductions in crime. In Boston, Massachusetts, the SPI strategy was associated with a 17.3 percent reduction in total violent crime, a 19.2 percent reduction in the number of robberies, and a 15.4 percent reduction in the number of aggravated assaults—with no evidence of displacement or diffusion effects. In Los Angeles, California, the Newton Division (persistently one of the city's most violent divisions) ended 2012 with an all-time low of 16 homicides following implementation of its SPI strategy. This was a 56 percent decrease compared to 2011 and 59 percent compared to 2010 in that division.

- ✓ In order to publicly recognize version 2.0 of the NCISP, it is recommended that the nation's law enforcement associations sign a national endorsement to demonstrate law enforcement's collective support.
- ✓ The CICC should support the development of outreach materials for version 2.0 of the NCISP that detail the importance of the revisions and how the NCISP benefits state, local, and tribal law enforcement agencies.

Recommendation: Law enforcement and homeland security agency executives should demonstrate their commitment to implementing the recommendations contained in the NCISP.

Action Items

- ✓ Law enforcement and homeland security executives should give serious consideration to implementing the recommendations of the NCISP, in coordination with their command staff, as agency capacity and resources allow.
- ✓ The CICC should support the development of guidelines, templates, and recommended metrics for use by agencies implementing version 2.0 of the NCISP.

Recommendation: Law enforcement agencies and organization executives should cultivate future leaders within their agency or organization as a means of strengthening the agency and succession planning.

Action Items

- ✓ Leaders should support national fellowship and leadership programs by sending individuals within their agency to participate and obtain the benefits that will support agency missions. Notable programs that should be considered are the FBI's National Academy and the DHS and FBI Fellows program.
- ✓ Leaders should take advantage of available leadership training courses that offer continuing education material for law enforcement executives. Notable programs that should be considered are the FBI's National Executive Institute and the Fusion Center Leaders Program (FCLP), hosted by the Naval Postgraduate School (NPS) Center for Homeland Defense and Security (CHDS).

Partnerships

Maintaining a superior level of service and/or exceeding expectations under limited resources can be challenging. Partnerships have become an effective means to confronting such obstacles, and they provide multiple agencies with solutions to overcome complex challenges. This section focuses on the importance of building partnerships with both law enforcement and non-law enforcement agencies and the value these partnerships have to all parties involved.

Recommendation: To sustain effective information sharing, it is imperative that law enforcement agencies continue to develop and enhance partnerships with each other, as well as with the private sector, other public safety disciplines, privacy advocates, and community groups, to foster collaboration and coordination that provide for improved public relations and may also support criminal intelligence development.

Action Items

- ✓ Law enforcement agencies should consider creating and implementing outreach strategies in order to develop and enhance partnerships with the private sector, non-law enforcement public safety disciplines, privacy advocates, and community groups.
- ✓ Law enforcement should understand vulnerabilities associated with critical infrastructure and key resources (CIKR). Partnerships with CIKR professionals need to be developed prior to situations (or emergencies) that necessitate assistance from either or both parties.
- ✓ Law enforcement agencies as well as federal partners should encourage the distribution and implementation of NSI training modules for current and potential private sector and non-law enforcement public safety partners.

Recommendation: Law enforcement agency personnel should participate with professional organizations.

Action Item

- ✓ Law enforcement agency personnel should build their own networks through professional organizations. Membership in professional organizations provides for professional development, continued education, relationship building, and the overall strengthening of the law enforcement community.

Getting Started

Partnerships

- > Become a member of a national law enforcement association.
- > Identify and partner with the state or major urban area fusion center.
- > Implement the tenets of the *Building Communities of Trust Initiative* to reach out and engage with community members.

Success Story

California State Threat Assessment Center (STAC)

The California State Threat Assessment Center (STAC) has faced numerous challenges and works diligently to produce the most timely and relevant intelligence possible. To improve STAC's analyses on terrorism, Mexican drug trafficking organizations, criminal extremists, gangs, and other areas, STAC has forged partnerships and other relationships that leverage different disciplines and sources of information. Among its most notable partnerships has been its collaboration with the California Department of Forestry and Fire Protection (CAL FIRE) on a joint intelligence bulletin that focused on ember bombs. The work on this bulletin was initiated as a result of an article published in *Inspire* magazine that included CAL FIRE's assistance with executing a practical test of the ember bomb at its training facility. STAC integrated the results of the tests into the joint intelligence bulletin and combined the data with the context of al Qaeda strategy in the United States. STAC's partnerships with state agencies, such as CAL FIRE, have resulted in groundbreaking assessments that not only painted an intelligence picture but also provided actionable information for law enforcement partners. Additionally, collaborations with federal agencies have established STAC as an intelligence producer in the federal space and ensured that the California perspective has reached the entire country.

Resource Spotlight

The NSI has developed ***Suspicious Activity Reporting Training for Hometown Security Partners*** training modules to assist in educating these disciplines on the importance of observing suspicious activity and reporting it to their chain of command, their local law enforcement agency, and their Fusion Liaison Officer (FLO), in accordance with their established policies and procedures.

This product would be a great tool to use in building a valuable partnership with a solid foundation and is available on the NSI Program Management Office Web site (http://nsi.ncirc.gov/training_online.aspx).

Additionally, the fusion center FLO program can assist with cross-training opportunities between disciplines, and law enforcement agencies should consider a partnership with a fusion center to participate in and/or help establish a FLO program.

Recommendation: Law enforcement agencies should continue to build partnerships with fusion centers.

Action Items

- ✓ Law enforcement agencies should utilize the Web site established by the U.S. Department of Homeland Security (http://www.dhs.gov/state-and-major-urban-area-fusion-centers) for information on state and major urban area fusion centers and should leverage the resources available for use by contacting the fusion center closest to their area of responsibility.
- ✓ Fusion centers should reach out to RISS and HIDTAs to build relationships with each organization in their region.

Resource Spotlight

The document ***Guidance for Building Communities of Trust*** provides advice and recommendations on how to initiate and sustain trusting relationships that support meaningful sharing of information, responsiveness to community concerns and priorities, and the reporting of suspicious activities that appropriately distinguish between innocent cultural behaviors and behavior that may legitimately reflect criminal enterprise or terrorism precursor activities. The guidance was developed in partnership with select sites that participated in the Nationwide SAR Initiative (NSI) Evaluation Environment and can be obtained online via the following link: http://nsi.ncirc.gov/BCOT-Guidance.

Success Story

Intelligence-Led Community Policing, Community Prosecution, and Community Partnerships (IL3CP)

Intelligence-Led Community Policing, Community Prosecution, and Community Partnerships (IL3CP) is a unique approach to community justice and public safety in the twenty-first century. It extends the basic concepts of community policing to include prosecutorial authority, community organizations, and intelligence-led operations. IL3CP blends the core elements of community policing with the corollary approaches of community prosecution. This new model strives to connect the criminal justice system and the community through seamless communication and partnerships to develop initiatives on a foundation of actionable intelligence.

IL3CP is built on the established organizational structure of the Rockland County, New York, District Attorney's Office (RCDAO). Since the implementation of IL3CP, Rockland County has realized reductions in serious crime—dramatic in several offense classes—as well as improvements in addressing basic community issues. The RCDAO also partnered with the International Association of Chiefs of Police (IACP) to conduct an assessment of IL3CP. With funding from the COPS Office, RCDAO and IACP personnel implemented the model in three cities across the United States: Mesa, Arizona; Newport News, Virginia; and St. Paul, Minnesota. The following year, IACP personnel conducted an assessment of the IL3CP projects in each pilot city to determine their impact on crime and community safety. The results of that assessment will be published in a report from the COPS Office in late 2013. Additional information is available through IACP and the Rockland County District Attorney's Office.

As a part of their mission to protect the public and property, law enforcement personnel must also ensure the protection of privacy, civil rights, and civil liberties (P/CRCL) for those they serve. The NCISP has included P/CRCL protections as a critical element to emphasize the importance of these protections in the implementation of the NCISP.

Recommendation: Law enforcement and homeland security agencies should maintain a strong emphasis on the protection of privacy, civil rights, and civil liberties (P/CRCL) in all law enforcement and homeland security actions and operations.

Action Items

- ✓ All law enforcement and homeland security agencies should develop a privacy policy and ensure that the tenets of the policy are implemented.
- ✓ Law enforcement and homeland security agencies should develop and/or enhance existing agency policies that may have P/CRCL implications (such as social media use, First Amendment-protected demonstrations).
- ✓ Agencies should consider, as a best practice, performing a Privacy Impact Assessment in order to uncover the privacy risks and vulnerabilities within their information sharing system.

Getting Started

Privacy, Civil Rights, and Civil Liberties Protections

- > Develop a privacy policy using the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (Privacy Guide).
- > Train agency personnel on privacy protections using *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety* online training.

- ✓ The CICC should support efforts to work with the Commission on Accreditation for Law Enforcement Agencies (CALEA) and state accrediting bodies to incorporate language into the appropriate standards requiring agencies to have privacy policies. These policies should include activities related to the intelligence function.
- ✓ The CICC should support efforts to develop a template for law enforcement executives to use in educating the public on the efforts of law enforcement to preserve the P/CRCL of the communities they serve, thereby improving agency transparency.
- ✓ All law enforcement officers should receive annual training on P/CRCL protections, as related to their duties and responsibilities.

Recommendation: Law enforcement agencies should consider adopting the privacy principles promoted by Global and the CICC, and the CICC should continue to support the development of guides and templates that facilitate policy development and compliance.

Action Item

- ✓ Law enforcement agencies should utilize the templates recommended by the CICC to ensure that their policies meet the minimum national standards for protecting the privacy, civil rights, and civil liberties of their community members.

Resource Spotlight

The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety training video assists state, local, and tribal law enforcement frontline officers in understanding their role in the protection of privacy, civil rights, and civil liberties (P/CRCL) as they perform their everyday duties.

The video provides an introductory overview of what P/CRCL protections are, examples of these protections, and the important function line officers have in upholding these protections.

The short video may be used during roll call and in-service training, incorporated into agency distance-learning capabilities, and used to complement other agency privacy-related training efforts. This video can be viewed online via the NCIRC Web site: http://www.ncirc.gov/privacylineofficer/.

Success Story

First Amendment-Protected Events for State and Local Law Enforcement Agencies

Following the influence of the Occupy Movement that began in New York, a group called "Occupy Minnesota" began to set up an encampment on Hennepin County property. After the onset of these events, reporting on the group's activities within the Hennepin County Sheriff's Office and communicating with its state and local law enforcement partners became increasingly difficult. In an effort to assist state and local law enforcement with these types of events, the CICC developed a guide entitled ***Recommendations for First Amendment-Protected Events for State and Local Law Enforcement Agencies***. The guide gave the Hennepin County Sheriff's Office a better understanding of how to disseminate information without infringing on citizens' First Amendment rights.

The comprehensive guide, which includes a breakdown of the Pre-Event Stage, the Operational Stage, and the Post-Event Stage of First Amendment-protected events, became a valuable resource in handling the ongoing events. The guide was shared officewide, and key portions were read at roll calls to deputies providing public safety at the encampment site and surrounding Hennepin County properties. Included in these sections were the "Red Flags," which laid out the importance of how information was gathered and disseminated. With the use of this guide, the Hennepin County Sheriff's Office was able to appropriately protect the First Amendment rights of the groups involved while continuing to ensure public safety.

Policies, Plans, and Procedures

Agencies and organizations should have policies, plans, and procedures in place to ensure effective and efficient operations and fulfillment of agency missions. Policies, plans, and procedures also protect agencies and organizations from undue harm and reduce risk. This section details how agencies can address internal operations and will help ensure a level of consistency nationwide among policies, plans, and procedures that address all crimes and terrorism. These common policies, plans, and procedures will also facilitate the development and sharing of criminal intelligence and the sharing of information.

Recommendation: Agencies should follow the tenets of 28 Code of Federal Regulations (CFR) Part 23 regarding the collection/submission, access or storage, and dissemination of criminal intelligence information by law enforcement agencies while conforming to the privacy and constitutional rights of individuals, groups, and organizations.

Action Items

- ✓ Law enforcement agencies should consider adopting the standards required by 28 CFR Part 23, regardless of whether or not an intelligence system is funded by the U.S. Department of Justice.
- ✓ All agency personnel involved in the intelligence function should undergo regular 28 CFR Part 23 training (https://www.ncirc.gov/28cfr/Default.aspx).

Resource Spotlight

28 CFR Part 23 training (https://www.ncirc.gov/28cfr/Default.aspx) can be accessed on the secure NCIRC Web site through the Regional Information Sharing Systems Network (RISSNET™), Law Enforcement Online (LEO), or the Homeland Security Information Network (HSIN).

Recommendation: The CICC should promote the use of the IACP's Criminal Intelligence Model Policy (2003 revision) (http://www.ncirc.gov/documents/public/criminal_intelligence_model_policy.pdf) and the Association of Law Enforcement Intelligence Units (LEIU) *Criminal Intelligence File Guildelines* (http://www.ncirc.gov/documents/public/criminal_intel_file_guidelines.pdf) and develop products supporting these resources, as appropriate.

Getting Started

Policies, Plans, and Procedures

- > Direct appropriate agency personnel to take the 28 CFR Part 23 online training course.
- > Create and implement a policy on the collection, analysis, and dissemination of intelligence using the IACP's Criminal Intelligence Model Policy and the LEIU *Criminal Intelligence File Guildelines* into the agency's intelligence process.

Action Items

- ✓ Law enforcement and homeland security agencies should consider implementing the IACP's Criminal Intelligence Model Policy (2003 revision) and the LEIU *Criminal Intelligence File Guidelines* as a part of their intelligence capability.
- ✓ The CICC should support the development of guidance and a template for law enforcement agencies who desire to have an intelligence collection capability.

Intelligence Process

The impact of 800,000 law enforcement officers contributing to the intelligence process has the potential to crush crime. That collective force could provide an unmatched level of safety and security to communities nationwide. To the extent possible, every law enforcement agency should have an intelligence capability; agencies that participate in the intelligence process stand to gain considerable value and significantly improve their crime reduction efforts, regardless of depth of implementation. This critical element reinforces the need to participate in the intelligence process. Regardless of agency size or resources, the use of intelligence-led policing can help agencies allocate patrols, improve investigations, enhance community response, and increase agency effectiveness.

Recommendation: Law enforcement and homeland security agencies should include prevention of crime as a top priority in agency mission and resource allocation, which will also support the implementation of the core capabilities in the *National Prevention Framework*, available at: http://www.fema.gov/media-library/assets/documents/32196?id=7358.

Action Item

- ✓ As stated in the NCISP, all law enforcement agencies should participate in terrorism and crime prevention activities by establishing an intelligence capability in their operations, partnering with their respective state or major urban area fusion center, adopting intelligence-led policing (ILP) processes, and supporting effective response for disasters and incidents.

Recommendation: Every law enforcement agency should take part in the intelligence process.

Action Items

- ✓ Law enforcement agencies should understand and develop a plan for the collection, identification, and sharing of information needs, as related to criminal intelligence.

Getting Started

Intelligence Process

- > Identify the top threats in the jurisdiction to then develop a collection plan that addresses the threats.
- > Develop a suspicious activity reporting (SAR) process for the agency.
- > Assign an officer to serve as a liaison to the fusion center.
- > Incorporate analysis into law enforcement operations via hiring of an analyst or partnership with a fusion center.
- > Incorporate an event deconfliction system into agency operations.

Observing and Reporting Suspicious Activity Information: A Call to Action

As a law enforcement or homeland security professional, you are responsible to ensure that the public you serve understands how to report suspicious activity and that your agency/organizational members support the collection, analysis, and submission of suspicious activity reports to your fusion center or the FBI/JTTFs. This "call to action" was agreed upon by law enforcement associations across the country. (http://nsi.ncirc.gov/documents/A_Call_to_Action.pdf)

Liaison Officers

Fusion Liaison Officer (FLO)—Fusion Liaison Officers are individuals who serve as the conduit for the flow of homeland security and crime-related information between the field and the fusion center for assessment and analysis. FLOs can be from a wide variety of disciplines, can provide the fusion center with subject-matter expertise, and may support awareness and training efforts. Fusion centers may use various names for FLOs, such as Terrorism Liaison Officer, Intelligence Liaison Officer, and Field Intelligence Officer.

- ✓ Fusion centers and larger agencies that employ intelligence analysts or have an established intelligence function should reach out to smaller agencies and potential partners in their region and discuss opportunities to collaborate and help meet the needs of local law enforcement.

Recommendation: Law enforcement agencies should be educated in the area of Incident Management, including the role of the intelligence/investigation function. At any time, any law enforcement agency can be confronted with a major incident that may require the establishment of a command structure overseeing many aspects to command and control the incident. Such a command structure may include many diverse agencies from state, local, tribal, and federal governments. The flow of information and Intelligence is vital to achieve success in addressing these incidents.

Action Item

- ✓ Law enforcement agencies should have their department's intelligence function structured and trained to become an active participant in addressing incidents. For assistance in preparing for such events, the National Incident Management System (NIMS) *Intelligence/Investigations Function Guidance* document should be consulted.

Recommendation: All law enforcement and homeland security agencies should implement a suspicious activity reporting process and participate in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI).

Action Items

- ✓ Agencies should develop and implement a process to actively collect suspicious activity reports.
- ✓ Agencies should develop a process for routing suspicious activity report information as quickly as possible after it has been received to ensure that the FBI Joint Terrorism Task Forces (JTTFs) evaluate and investigate SARs.
- ✓ All law enforcement agencies should develop a policy (or similar guidance document) regarding the SAR process that will address implementation, privacy, partnerships, training, community outreach, and technology.
- ✓ Agencies should train their officers and coordinate the training of public safety partners (dispatchers, emergency managers, firefighter and EMS personnel, etc.) on how to identify and report suspicious activity using the training modules developed by the

Hot-Spot Policing

Research has shown that place-based enforcement efforts, frequently referred to as "hot-spot policing" initiatives, along with other evidence-based practices, offer the best results to reduce and prevent crime.

—National Institute of Justice, 2009

NSI Program Management Office (PMO) (available on the NSI Web site: http://nsi.ncirc.gov/training_online.aspx).

Recommendation: Law enforcement agencies at all levels of government should establish a working relationship with their respective state or major urban area fusion center.

Action Items

- ✓ State, local, and tribal law enforcement agency leadership should establish and institutionalize procedures to accomplish the sharing of information and criminal intelligence with their applicable state or major urban area fusion centers, and those efforts should be reciprocated. In addition, state, local, and tribal law enforcement agencies should develop policies and procedures to ensure the continued dissemination of information and intelligence provided by the applicable fusion center to their appropriate agency staff members.
- ✓ Local police departments should communicate their information needs to their fusion center, further supporting the fusion center's goal of meeting state, local, and tribal information needs.
- ✓ State and major urban area fusion centers should have an established outreach and communications plan that incorporates all applicable agencies, organizations, and homeland security partners within their jurisdiction or area of responsibility. The plan should describe the fusion center's capabilities and discuss what the center can offer its federal, state, local, and tribal public safety and private sector partners.
- ✓ Public safety agencies should identify a liaison officer(s) to assist in coordinating the agency's intelligence, fusion, and/or multidisciplinary efforts.

Recommendation: Law enforcement agency leadership should recognize the value of the analytic component and utilize this component to the degree appropriate, considering the size of the agency and its available resources.

Action Items

- ✓ Smaller agencies that do not have the capacity to develop and sustain an analytic function should partner with regional information and intelligence centers and state or major urban area fusion centers.
- ✓ Analysts should participate in applicable training opportunities to further develop and refine their analytic capabilities.
- ✓ Agency leadership should emphasize the professionalization of their analytic staff through training, membership in professional organizations, and networking and collaboration with appropriate partners.

Understanding the Difference

Crime Analysis: A type of analysis that uses a set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist operational and administrative personnel in planning the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and increasing apprehensions and the clearances of cases.[5]

Intelligence Analysis: A type of analysis that uses the scientific approach to problem solving to develop a product that provides an integrated, actionable assessment of crime trends, crime and security threats, and conditions that describe changes in the criminal threat picture (synonymous with criminal intelligence analysis).[6]

Additional discussion for further clarification: Crime analysis focuses on analyzing a series of crimes—most notably homicide, assault, robbery, burglary, and auto theft—that have already occurred, with the intent of apprehending the offender(s) and deterring continued criminal acts. Conversely, intelligence analysis assesses diverse types of information that suggest potential criminality—such as suspicious activity reports, tips, and leads—for the purpose of identifying a criminal threat that is typically transjurisdictional in nature, with the purpose of intervening to stop the threat.

Success Story/Emerging Issue
School Violence Initiative (SVI)

The Southern Nevada Counter-Terrorism Center (SNCTC) School Violence Initiative (SVI) was developed by the SNCTC in response to the murder of a 16-year-old honor roll student and athlete who was shot and killed while walking home from school. The perpetrators, who were later tried and convicted of murder, were known associates of a local gang. Shortly after the shooting, SNCTC crime analysts conducted an intensive analytic study of the empirical data surrounding previous school shootings, existing police tactics, strategies, and protocols and found that several calls for service or reports from students, parents, or school administrators typically preceded each event. However, this information was not being collected in a systematic way and was not being quickly disseminated to first responders.

The SNCTC SVI was created as a result of a complex and calculated analytic approach to curbing school violence and was designed to improve the collection, management, and dissemination of intelligence-related school violence information throughout the law enforcement community in southern Nevada. Analysis revealed several weaknesses with existing law enforcement techniques related to school violence, such as misplaced resources resulting from flawed assumptions that all school shootings were gang-related, information silos that prevented law enforcement agencies from sharing information critical to preventing violent activity, and a lack of accountability and coordination for disseminating information. As a result of these findings, the SNCTC Crime Analysis Manager spearheaded a collaborative effort among the Clark County School District Police Department (CCSDPD), the Las Vegas Metropolitan Police Department, the Henderson Police Department, and the North Las Vegas Police Department. The partnership between the organizations led to the official launch of the SVI, in which nine intervention techniques were implemented to reduce school-related violence. Implementation of the intelligence process by SNCTC was instrumental in reducing misplaced resources through access to better data, eliminating information silos, and improving multiagency coordination efforts.

Also critical to the success of the SVI was embedding a full-time CCSDPD liaison representative within SNCTC. The position gave the CCSDPD representative access to multiagency criminal databases and real-time incident management systems, thus allowing fluid critical communication and increased response time to deter potential violent activity. Since the SVI was launched, there have been ZERO school shootings in the Las Vegas valley. The SVI has been a tremendous success.

Recommendation: Personnel involved in the intelligence function should be knowledgeable of the sources of information, to include new and emerging resources, and their applicability to the development of criminal intelligence.

Action Items

- ✓ Law enforcement personnel should continually identify sources of information to utilize in criminal intelligence and information development, including agency reports, social media resources, and information from other public safety partners.
- ✓ As law enforcement agencies integrate social media resources and information into the criminal intelligence process, they should develop a social media policy, articulating the privacy, civil rights, and civil liberties protections associated with the use of social media sites.

Recommendation: Law enforcement agencies should understand and develop a plan to participate in the Criminal Intelligence Enterprise (CIE). This plan should involve the development of prioritized threat domains, collection on respective threats, analysis, and dissemination as related to criminal intelligence and information sharing.

Action Item

- ✓ Law enforcement leaders who have a dedicated criminal intelligence component should engage in the standardized process identified in the MCCA Criminal Intelligence Enterprise initiative to develop their threat domain assessment, collection plan, and information needs.

Recommendation: Law enforcement and homeland security agency executives should be engaged in the intelligence process to ensure awareness of emerging issues.

Action Items

- ✓ Law enforcement agency executives should become members of their regional, state, and national information sharing groups and associations in order to be apprised of and raise critical emerging issues and learn about effective strategies to address them.
- ✓ Agency executives should be responsible for outreach to and collaborative efforts with their fusion center.
- ✓ Law enforcement executives should maintain their involvement with emerging areas of the law, including privacy-related issues and criminal intelligence development, storage, and retention requirements.

Criminal Intelligence Enterprise (CIE)

The Criminal Intelligence Enterprise (CIE) is a national initiative led by the Major Cities Chiefs Association (MCCA). It is composed of two key objectives: (1) increase the connectivity among local intelligence units and (2) institutionalize a standardized assessment process that enables each agency to better identify and measure its priority threat groups, establish actionable information needs, an develop more focused intelligence collection plans. Additional information on the CIE is available at https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_ntelligence_enterprise_initiative_20120329.pdf.

Resource Spotlight: Social Media Policy Guidance

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations: http://www.it.ojp.gov/gist/document/132.

Resource Spotlight

Line Officer SAR Training—The SAR Line Officer Training was developed to assist law enforcement frontline officers in understanding what kinds of suspicious behaviors are associated with pre-incident terrorism activities, documenting and reporting suspicious activity, and protecting privacy, civil rights, and civil liberties when documenting information. This training also provides information about integrating the Nationwide SAR Initiative (NSI) into an agency's operations. Available at: http://nsi.ncirc.gov/training_online.aspx.

Line Officer Privacy Training—*The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety* training video was developed through a partnership effort led by the Bureau of Justice Assistance (BJA) to assist state, local, and tribal law enforcement frontline officers in understanding their role in the protection of privacy, civil rights, and civil liberties as they perform their everyday duties. The video provides an introductory overview of what privacy, civil rights, and civil liberties protections are; examples of these protections; and the important function frontline officers have in upholding these protections. Available at: http://www.ncirc.gov/privacylineofficer/lineofficer.swf.

Analytic Training Standards—The Analytic Training Standards identify recommended minimum objectives and standards for analyst training. The goal of the standards is to provide supervisors, analysts, and training partners with a common set of training criteria, thereby creating a more uniform analyst profession.

Recommendation: A continued emphasis should be placed on the need for the declassification and wide dissemination of classified documents for law enforcement purposes, with the sensitive source and method-of-collection data redacted, yet retaining as much intelligence content as feasible.

Action Items

- ✓ All law enforcement and homeland security agencies should develop products at the lowest possible level of classification to promote dissemination to the widest audience possible.
- ✓ Unclassified versions of products should be developed whenever possible to promote expanded sharing of information to relevant audiences that may not have clearances.

Training

As their environment changes, law enforcement and homeland security officials must meet new challenges head-on. Meeting these challenges requires training, which helps ensure the safety of both the officers in the field and those they serve, while maintaining effective policing strategies. This section discusses training components and the avenues needed (such as distance-learning platforms) to implement the tenets of the NCISP.

Recommendation: In order to fully implement the tenets of the NCISP, law enforcement agency leadership should ensure that personnel receive training on the intelligence process and privacy issues associated with the intelligence process.

Action Items

- ✓ Law enforcement officers should complete the national-level courses pertaining to the intelligence process and related privacy implications either through in-service training or through their basic/entry-level training.
- ✓ The National Criminal Intelligence Resource Center (www.ncirc.gov) should be utilized to provide law enforcement agency personnel with a comprehensive listing of and access to criminal intelligence-related training programs and resources.
- ✓ The creation of a national distance-learning platform should be considered to cost-effectively expand the delivery of criminal intelligence training to law enforcement professionals across the country.
- ✓ The CICC should continue to support efforts with the International Association of Directors of Law Enforcement Standards and Training and the IACP State and Provincial Police Academy Directors section as well as other training organizations in order to continue to promote and implement the recommended NCISP training standards in every state.
- ✓ Federal partners should consider including national training requirements in grant guidance.
- ✓ The CICC should develop a road map for analyst training.

Getting Started

Training

> Access the National Criminal Intelligence Resource Center to identify training opportunities (both online and via the Criminal Intelligence Training Master Calendar available at: http://mastercalendar.ncirc.gov.

> Utilize the standards identified in the *Minimum Criminal Intelligence Training Standards* when finding training opportunities for law enforcement personnel, including analysts (https://it.ojp.gov/gist/108/Minimum-Criminal-Intelligence-Training-Standards).

> Incorporate basic training on intelligence into in-service training.

Security and Safeguarding

Law enforcement and homeland security agencies have a great deal invested in their mission to protect the communities they serve. These agencies make a substantial investment in information management and data communications technologies to better enable this mission. These investments add inherent vulnerabilities that must be managed to ensure the security of systems, networks and information. Further, in recognition of the goals illustrated in version 2.0 of the NCISP, to enhance information and intelligence sharing across jurisdictions, organizations, and levels of government, information security must be a priority.

Information sharing and interoperability require that connections between consumers and providers of information be opened. Therefore, the implementation of stringent security measures, operational and technological, utilizing national standards and best practices is imperative. This section elaborates on the security initiatives and resources available to law enforcement and homeland security agencies to assist them in the adoption and use of information sharing and safeguarding standards to protect their information sharing environments from cyber attack and also offers guidance in the area of security clearances.

Recommendation: Law enforcement agencies should understand and continue to educate themselves on cybersecurity risks affecting the management and sharing of information and criminal intelligence.

Action Items

- ✓ The CICC should support and promote the dissemination of resources developed by state, local, and federal partners pertaining to emerging security threats that detail how agencies can minimize their vulnerabilities and protect themselves from security threats.
- ✓ State and local law enforcement should consider engaging with DHS Cyber Security Advisors (CSAs) to bolster their cybersecurity preparedness, risk mitigation, and incident response capabilities in an effort to increase the resiliency of their cybersecurity infrastructures.
- ✓ Law enforcement agencies should consider the implementation of security practices recommended by the Global Standards Council, such as an access control mechanism based on Global Federated Identity and Privilege Management (GFIPM) and the guidelines defined in the Global Technical Privacy Framework.
- ✓ Law enforcement agencies should adhere to the rules of the FBI CJIS Security Policies—in particular, CJIS encryption requirements (for data exposed while in transit [i.e., over the Internet]).
- ✓ Law enforcement agencies should conduct a self-assessment of their internal systems and strengthen their systems as needed to prevent intrusions and internal leaks of information.

Getting Started

Security and Safeguarding

> Participate in national system monitoring networks, such as the Multi-State Information and Analysis Center (MS-ISAC).

> Adhere to the rules of the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policies.

Recommendation: Security clearances should be equally recognized by all government agencies in order to provide increased collaboration and access to information and intelligence.

Action Items

- ✓ The CICC and its law enforcement partners should continue to support Executive Order 13549 and its implementing directive (more specifically, Section 1.3(c), which states, "All clearances granted to SLTPS [state, local, tribal, and private sector] personnel, as well as accreditations granted to SLTPS facilities without a waiver, shall be accepted reciprocally by all agencies and SLTPS entities").
- ✓ Federally issued security clearances should be recognized and issued to local law enforcement to provide for a "surge" capacity of police officers and deputies who are fully cleared and are regularly briefed on national security and criminal investigations and prepared to assist the federal partners (including the FBI) as needed in investigative activity.

Resource Spotlight

Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies—A Guide for Executives, Managers, and Technologists (http://www.search.org/files/pdf/ITSecTechGuide.pdf) can be utilized by law enforcement to raise awareness of information security risks and better protect themselves from related threats. This document is intended to provide the law enforcement community with strategies, best practices, recommendations, and ideas for developing and implementing information technology security policies. It will help agencies identify and assess internal information technology security risks and provide ideas for mitigating them.

Technology and Standards

Technology is ever-changing, which provides both opportunities and obstacles for law enforcement agencies as they build and enhance their criminal intelligence and information development and sharing processes. Standards help minimize obstacles and, to some degree, help extend the lifelines of some technology products (such as legacy systems). This section addresses some of the obstacles that may result from technological advances and offers recommendations on how to address these obstacles. Furthermore and more specifically, this section focuses on how to simplify the access to and sharing of information across various systems.

Recommendation: In alignment with the NCISP, it is recommended that national information sharing standards, based upon those widely adopted by government and industry, be utilized by law enforcement agencies to reduce unnecessary (and potentially wasteful) variations in technology solutions and improve information sharing.

Action Item

- ✓ The standards described in the following paragraph will provide a foundation for the effective development of information sharing capabilities to support version 2.0 of the NCISP. Each has been developed for use by law enforcement, fusion centers, and the broader criminal justice and public safety community. These standards are being used by law enforcement agencies across the country. [continued on page 34]

Getting Started

Technology and Standards

- > Gain access to a Sensitive but Unclassified (SBU) system (Regional Information Sharing Systems Secure Cloud [RISSNET], Law Enforcement Online [LEO], Homeland Security Information Network [HSIN] or Intelink-U).
- > Implement the Global Federated Identity and Privilege Management (GFIPM) framework in your agency.
- > Ensure that your agency's technologists are using the National Information Exchange Model (NIEM) and its "data vocabulary" in their data exchanges across sytems.

Success Story

NIEM Facilitates Gang Data Sharing

State, local, and regional law enforcement and public safety agencies in Massachusetts lacked an effective mechanism to capture and share gang-related data statewide. Gang data was stored and maintained locally in agency-specific electronic and paper-based systems that did not support effective information sharing across jurisdictions. To address this challenge, a centralized repository and Web-based gang data management application called MassGangs was implemented by the Massachusetts Executive Office of Public Safety and Security. MassGangs is an intelligence and investigative tool that allows authorized users to electronically exchange, store, and facilitate the analysis of gang-related data maintained by public safety and law enforcement agencies throughout Massachusetts. MassGangs promotes the real-time sharing of gang and gang member information across various state, local, and regional public safety partners. The project promotes enhanced public safety and security in Massachusetts by enabling statewide access and cross-agency gang data sharing for more than 370 law enforcement and criminal justice agencies. By using NIEM in the MassGangs project, the commonwealth has streamlined the gang data management process, providing a single, unified way for agencies to share gang intelligence information within Massachusetts.

- Strong consideration should be given to utilization of the National Information Exchange Model (NIEM) as the common data vocabulary for exchanging data across systems and data management environments. NIEM is a national standard for data exchange, having now been adopted by 15 U.S. government domains.
- Strong consideration should be given to utilization of the Global Reference Architecture (GRA), which provides the framework for interconnecting system and data environments and for orchestrating Web Services to move data between environments by supporting an expanse of information sharing methods. It is the interoperability layer.
- Strong consideration should be given to utilization of the the Logical Entity Exchange Specification (LEXS), which provides the ability to package NIEM services using consistent definitions supporting publication, search, and retrieval that are fundamental to information sharing.
- Strong consideration should be given to utilization of the the Global Federated Identity and Privilege Management (GFIPM) framework, which provides the overarching structure for secure single sign-on to the networks, data sources, applications, and technologies utilized by law enforcement. It also is the underlying standard for ensuring the authentication of access and privilege within an information sharing federation where a variety of technologies and standards need to coexist.
- These standards will help to accelerate the advancement of the information sharing solutions supporting the NCISP. Today, there are GFIPM-based solution alternatives for agencies to consider.

Success Story
The Indiana Data Exchange (IDEx) Project

The Indiana Data Exchange (IDEx) Project is a 21-agency effort under the leadership of the Indiana Department of Homeland Security that includes state, local, and federal agency participation. The initiative connects disparate justice and public safety systems' data, leveraging existing investments for enhanced decision making and increased public safety by using a range of U.S. Department of Justice-supported solutions, including the GRA, GFIPM framework, and NIEM. Because the planning, design, and initial capital investment were grant-funded, IDEx exemplifies how a state can use federal support to initiate a project resulting in immediate and long-term cost savings and efficiencies.

Recommendation: Simplified user access and functionality across multiple systems should be developed to facilitate information access and sharing.

Action Items

- ✓ All law enforcement agencies should have access to at least one of the major sensitive but unclassified (SBU) systems (RISSNET, LEO, HSIN, or Intelink).
- ✓ Federal partners should work toward enhanced interoperability between SBU systems.
- ✓ Law enforcement agencies adopting new forms of information sharing technology should maximize and leverage the existing information sharing networks, standards, and applications before developing new ones. If new information sharing capabilities need to be developed, it is recommended that agencies consider the concept of joining a federated ISE to accelerate and economize information sharing and interoperability with key systems (RISSNET, LEO, HSIN, Intelink).
- ✓ The CICC and its partner agencies should support efforts to simplify user access to SBU systems.
- ✓ The CICC should support continued efforts aimed at "single sign-on" and federated search.

Recommendation: Law enforcement agencies at all levels of government should participate in deconfliction using existing technology solutions to ensure both officer safety and increased interagency coordination.

Action Items

- ✓ All law enforcement agencies should participate in an event deconfliction system to enhance officer safety.
- ✓ Law enforcement agencies should incorporate target and subject deconfliction systems as a part of standard agency protocol.

A Call to Action: Enhancing Officer Safety Through the Use of Event Deconfliction Systems

Event deconfliction is the process of determining whether law enforcement personnel are conducting an enforcement action (e.g., a raid, an undercover operation, or surveillance) in proximity to one another during a specified time period. To implement systematic deconfliction into agency operations, agencies should utilize one of three nationally recognized event deconfliction systems: Case Explorer, RISSafe™, or SAFETNet. For additional information on event deconfliction and the "Call to Action," please visit: www.it.ojp.gov/event-deconfliction.

Sustainability

Sustainability is critical to the longevity of any agency or initiative. Sustainability ensures that the lifeblood and resources of an agency or initiative remain healthy enough for operations to continue. Sustainability plans may come in all shapes and sizes and will vary greatly depending upon things such as mission, type of service, and level of service delivered. This section focuses on the need for sustainability planning to help ensure longevity for the participants in the NCISP's Framework as well as the NCISP itself.

Recommendation: All partners supporting the implementation of the NCISP should consider supporting efforts to continue its implementation across all levels of government.

Action Items

- ✓ The CICC, in conjunction with the major law enforcement and homeland security organizations, should support development of a template for performance measurement plans designed specifically for law enforcement criminal intelligence programs. This template should address criminal intelligence sharing in order to credibly and objectively demonstrate programs' value and provide justification for the receipt of future resources.
- ✓ Federal agencies should consider building tenets of the NCISP into grant guidelines.
- ✓ Law enforcement should reach out to and educate government officials about the role of the intelligence function within the agency.

Best Practice—Fusion Center Assessment

The U.S. Department of Homeland Security (DHS), in coordination with the National Network of Fusion Centers and federal interagency partners, conducts an annual assessment that evaluates the progress made by individual fusion centers in achieving Critical Operational Capabilities and Enabling Capabilities and evaluates the performance of the National Network. Data collected through the assessments allows fusion centers to identify areas that are in need of improvement in order to strengthen capabilities and improve performance. Furthermore, having a defined assessment and evaluation process that culminates in an official report will help drive federal support for fusion centers.

Appendix A—Endnotes

1 Intelligence—The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being or known to be criminal in nature. (Quoted in IACP, 1985, p. 5, from National Advisory Committee on Criminal Justice Standards and Goals, Organized Crime, 1976, p. 122) Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. (IACP National Law Enforcement Policy Center, 1998).

2 Within the context of this document, intelligence capability also refers to the agency's willingness to implement those acts, within the intelligence process or cycle, that it is capable of performing.

3 Additional information on the National Network of Fusion Centers is available at http://www.dhs.gov/state-and-major-urban-area-fusion-centers and http://www.nfcausa.org.

4 Additional information on the NSI is available at http://nsi.ncirc.gov.

5 Gottlieb, Steven, Raj Singh, and Shel Arenberg. *Crime Analysis: From First Report to Final Arrest*. Alpha Publishing, 1995.

6 Carter, David L. (2009) *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. 2d ed. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.

Appendix B—Resources

To request copies of any of the following documents, please send an e-mail with the name of the document, the quantity requested, and your shipping address to: it@it.ojp.gov.

Critical Element 1: Leadership

National Strategy for Empowering Local Partners to Counter Violent Extremism in the United States
www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf

The Police Chief magazine, "The IACP Testifies on 'Going Dark'"
www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=2351&issue_id=42011

Critical Element 2: Partnerships

NSI Hometown Security Partners Training
http://nsi.ncirc.gov/training_online.aspx

Guidance for Building Communities of Trust
http://nsi.ncirc.gov/documents/e071021293_BuildingCommTrust_v2-August%2016.pdf

Critical Element 3: Privacy, Civil Rights, and Civil Liberties Protections

28 CFR Part 23 Online Training
Access the secure NCIRC Web site through RISSNET, LEO, or HSIN.

Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities: Privacy Guide
https://it.ojp.gov/gist/Document/31

Association of Law Enforcement Intelligence Units (LEIU) Criminal Intelligence File Guidelines
http://www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf

Global Privacy Resources document: Guide to Conducting Privacy Impact Assessments for State, Local, and Tribal Justice Agencies
www.it.ojp.gov/pia_guide

Justice Information Sharing Web site
http://it.ojp.gov/privacyresources

IACP Criminal Intelligence Model Policy
http://www.ncirc.gov/documents/public/supplementaries/criminal_intelligence_model_policy.pdf

The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety line officer training video
http://www.ncirc.gov/privacylineofficer/

Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies
http://www.ncirc.gov/documents/public/supplementaries/law_enforcement_intelligence.pdf

Navigating Your Agency's Path to Intelligence-Led Policing
www.ncirc.gov/documents/public/Navigating_Your_Agency's_Path_to_Intelligence_Led_Policing.pdf

Critical Element 4: Policies, Plans, and Procedures

28 CFR Part 23 Online Training
Access the secure NCIRC Web site through RISSNET, LEO, or HSIN.

Critical Element 5: Intelligence Process

NSI Web page
http://nsi.ncirc.gov/

Critical Element 5 (continued)

SAR Line Officer and Hometown Security Partners Training videos
http://nsi.ncirc.gov/training_online.aspx

Suspicious Activity Reporting Process Implementation Checklist
http://www.it.ojp.gov/gist/Files/sar%20checklist.pdf

A Unified Message Regarding the Need to Support Suspicious Activity Reporting and Training
http://nsi.ncirc.gov/documents/A_Call_to_Action.pdf

Analyst Toolbox
http://it.ojp.gov/docdownloader.aspx?ddid=1284

Common Competencies for State, Local, and Tribal Intelligence Analysts
http://it.ojp.gov/docdownloader.aspx?ddid=1296

Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations
http://www.it.ojp.gov/gist

Fusion Center Map
http://www.nfcausa.org

IACP Center for Social Media
http://www.iacpsocialmedia.org/

Law Enforcement Analytic Standards
http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf

MCCA White Paper
https://www.majorcitieschiefs.com/

Open Source Center
www.OpenSource.gov

Privacy Impact Assessment Report for the Utilization of License Plate Readers
http://www.theiacp.org/LinkClick.aspx?fileticket=N%2bE2wvY%2f1QU%3d&tabid=87

A Unified Message Regarding the Need to Support Suspicious Activity Reporting and Training
http://nsi.ncirc.gov/documents/A_Call_to_Action.pdf

Critical Element 6: Training

Countering Violent Extremism (CVE) Training Guidance and Best Practices
http://www.dhs.gov/xlibrary/assets/cve-training-guidance.pdf

Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States
www.it.ojp.gov/docdownloader.aspx?ddid=1152

Critical Element 7: Security and Safeguarding

Global Security Products
http://it.ojp.gov/security-products

Law Enforcement Tech Guide for Information Technology Security: How to Assess Risk and Establish Effective Policies—A Guide for Executives, Managers, and Technologists
http://www.search.org/files/pdf/ITSecTechGuide.pdf

Critical Element 8: Technology and Standards

National Information Exchange Model (NIEM) Web site
www.niem.gov

Global Reference Architecture (GRA) Web page
http://www.it.ojp.gov/GRA

Global Federated Identity and Privilege Management (GFIPM) Web page
http://www.it.ojp.gov/GFIPM

Appendix C—Accomplishments

The following are accomplishments realized since the creation of the NCISP (version 1.0) in 2003. Accomplishments have been organized under the nine critical elements s as identified in version 2.0.

Critical Element 1: Leadership

The CICC was established in 2004 and includes membership from state, local, tribal, and federal law enforcement and homeland security agencies, as well as national-level professional organizations that combined represent over 18,000 law enforcement agencies and more than 800,000 officers across the nation. The CICC meets, at a minimum, twice a year to discuss criminal intelligence sharing initiatives and opportunities as well as challenges to information sharing. The CICC reports its yearly activities, initiatives, and products in the Bureau of Justice Assistance (BJA) Annual Report and the Global Annual Report. The products that the CICC has supported have been instrumental to law enforcement agencies across the nation in fortifying their policies and facilitating agency operations.

A national signing event was held on May 14, 2004. The U.S. Attorney General and top law enforcement and homeland security officials attended the event, demonstrating their support for the NCISP. Upon the release of the NCISP, outreach materials were developed and provided to members for outreach to national law enforcement conferences, including the International Association of Chiefs of Police and the National Sheriffs' Association.

Critical Element 2: Partnerships

The CICC and GIWG supported the development of the *Fusion Center Guidelines* in 2006. The purpose of the guidelines initially was to provide guidance to law enforcement agencies on the development and operation of a fusion center. These guidelines were then expanded to include the involvement of public safety and private sector entities in fusion centers.

The CICC and Global also support the DHS/DOJ Fusion Process Technical Assistance Program, which provides training and technical assistance to fusion centers to ensure the development of a national integrated network of fusion centers. Tools and resources have been developed under this program to assist in both reaching out to the public and private sectors and incorporating them into fusion centers.

The CICC supported the development of the *Law Enforcement Analyst Certification Standards*, which promotes membership in a professional analyst association or organization.

Critical Element 3: Privacy

Many initiatives have been promulgated to ensure that the law enforcement community protects individuals' privacy and constitutional rights within the intelligence process. The *Fusion Center Guidelines* document includes a guideline emphasizing the need to protect privacy and civil liberties, the *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project* includes provisions regarding the protection of privacy and civil liberties, the training standards include sections on privacy, and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* document also addresses the importance of fusion centers having a privacy policy. The CICC has also partnered with federal agencies in initiating dialogue with privacy advocacy groups to discuss privacy issues related to criminal information and intelligence sharing.

The *Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise,* released in the spring of 2010, provides agencies with a process to ensure that their policies, procedures, and operating guidelines guarantee the protection of these rights.

A frontline officer training video entitled *The Importance of Privacy, Civil Rights, and Civil Liberties Protections in American Law Enforcement and Public Safety* was developed to assist agencies in training frontline officers on the importance of privacy, civil rights, and civil liberties protections in their day-to-day activities.

In the spring of 2010, fusion center privacy officials were trained on how to deliver privacy, civil rights, and civil liberties training to fusion center personnel.

The DHS/DOJ Fusion Process Technical Assistance Program includes technical assistance deliveries on the development of a fusion center privacy policy and is developing outreach resources for fusion centers when engaging law enforcement, public sector, and private sector entities.

In 2007, the CICC collaborated with the DHS/DOJ Fusion Process Technical Assistance Program in the development of the *Fusion Center Privacy Policy Development: Privacy, Civil Rights, and Civil Liberties Policy Template*. The template was designed to assist fusion centers in the development of a center privacy policy. The template incorporates the *Justice Information Privacy*

Guideline as well as the tenets of the Information Sharing Environment (ISE) Privacy Guidelines and 28 CFR Part 23.

Global also collaborated with BJA for the release of the *Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities* (Privacy Guide and Template), which provides a well-rounded approach to the planning, education, development, and implementation of agency privacy protections and further simplifies the process by including an easy-to-use development template.

Additionally, Global's Privacy and Information Quality Working Group has supported the development of many documents concerning the protection of citizens' privacy, civil rights, and civil liberties. These products can be located on the Justice Information Sharing Web site or can be searched through the Global Information Sharing Toolkit (GIST).

Critical Element 4: Policies, Plans, and Procedures

As a result of the release and dissemination of the NCISP, 28 CFR Part 23 has become the de facto standard for criminal intelligence databases for law enforcement agencies. Additionally, the CICC has played an active role in supporting the revisions of the regulation.

BJA developed 28 CFR Part 23 online training to assist agencies in efficiently and economically training personnel on the tenets of 28 CFR Part 23.

The CICC/Global Intelligence Working Group (GIWG) have recommended the IACP's Criminal Intelligence Model Policy (2003 revision) as a resource in documents and products, including the resource CDs for the NCISP and the *Fusion Center Guidelines*. This resource is also included in the Criminal Intelligence for the Chief Executive briefing and the Intelligence Commanders Course.

The CICC/GIWG have recommended the LEIU *Criminal Intelligence File Guidelines* document as a resource for inclusion in Global-supported documents, including in the resource CDs for the NCISP and the *Fusion Center Guidelines* as well as the *Baseline Capabilities for State and Major Urban Area Fusion Centers* document. This resource is also included in the Criminal Intelligence for the Chief Executive briefing and the Intelligence Commanders Course.

Critical Element 5: Intelligence Process

The Criminal Intelligence Coordinating Council (CICC) serves as an advocate for state, local, and tribal law enforcement and supports their efforts to develop and share criminal intelligence for the purpose of promoting public safety and securing the nation. The tenets of the NCISP are incorporated into all of the guidance and resources recommended and supported by the CICC and the GIWG.

After the NCISP was released, *10 Simple Steps to Help Your Agency Become a Part of the National Criminal Intelligence Sharing Plan* was released to provide solutions for agencies to implement the NCISP recommendations.

In April 2009, the CICC and GIWG supported the development of *Navigating Your Agency's Path to Intelligence-Led Policing*, designed to provide an overview and overarching guidance to agencies on how to implement the ILP framework.

The CICC supported collaboration with the Commission on Accreditation for Law Enforcement Agencies (CALEA) to enhance the accreditation program to include the tenets of the NCISP as they relate to criminal intelligence.

The *Law Enforcement Analytic Standards* was released in November 2004 and updated in 2011. Additionally, *Common Competencies for State, Local, and Tribal Intelligence Analysts* was released in 2010.

An acquisition mechanism or centralized site that enables law enforcement agencies to access shared data visualization and analytic tools has not been developed. However, the CICC supported development of the *Analyst Toolbox*, which provides a resource list of current products to assist analysts in effectively and efficiently performing their duties and producing useful intelligence products.

Critical Element 6: Training

The *Minimum Criminal Intelligence Training Standards* was released in 2004, and version 2.0 was released in 2007. These standards build on the core criminal intelligence training standards identified in the NCISP and provide perspective and guidance for the development and delivery of law enforcement intelligence training.

In June 2010, the *Common Competencies for State, Local, and Tribal Intelligence Analysts* was released, which provides a common set of core competencies for analysts working in law enforcement and intelligence-related environments. Training programs should also assess their analyst programs to ensure that these competencies are met.

Additionally, the CICC and GIWG support the DHS/DOJ Fusion Process Technical Assistance Program in the development and delivery of training and technical assistance for fusion centers.

The CICC continues to foster working relationships with law enforcement training organizations to ensure that the training standards set forth in the NCISP are met.

Critical Element 7: Security and Safeguarding

The CICC is involved in the Controlled Unclassified Information (CUI) Initiative, which will consolidate the numerous "markings" on documentation (including For Official Use Only, Law Enforcement Sensitive, Sensitive But Unclassified [SBU], etc.). As part of this initiative, the CICC was asked to represent the voice of state, local, and tribal law enforcement and homeland security agencies on how the CUI Framework will impact these agencies.

Many systems still do not require background checks. The trend is to allow law enforcement agencies access to SBU systems, with the understanding that each law enforcement agency conducts background checks on its personnel, whom they in turn approve for access to the SBU system.

Critical Element 8: Technology and Standards

Much work has been done in the development of standards and building of systems. BJA, in partnership with the IACP and the IJIS Institute, has developed the *Standard Functional Specifications for Law Enforcement Computer Aided Dispatch Systems (CAD)* and *Standard Functional Specifications for Law Enforcement Records Management Systems (RMS)* and, most recently, the *Unified CAD Functional Requirements* (police, fire, EMS). The specifications are designed to inform law enforcement about the basic functional requirements that all CAD and RMS systems should have in order to achieve interoperability.

Gaps still remain in the area of interoperability. Strides have been made in the development of networks such as the Homeland Security Information Network (HSIN) and the Homeland Security State and Local Intelligence Community of Interest (HS SLIC), but work still remains in achieving the desired level of system interoperability indicated in this recommendation.

The CICC continues to support the interoperability between RISS and LEO.

While a single solution has not been developed to ensure interoperability among the state, local, tribal, regional, and federal intelligence information sharing systems and repositories, Global has done some great work and has made significant progress towards achieving interoperability through such programs and initiatives as the Global Reference Architecture (GRA), the Global Federated Identity and Privilege Management (GFIPM), and the National Information Exchange Model (NIEM). New recommendations will continue to stress the importance of and the need for interoperability between intelligence systems.

On December 16, 2005, the President issued a memorandum regarding the Information Sharing Environment (ISE). Guideline 3 of this memorandum included Presidential direction to federal departments and agencies to recommend standardized SBU procedures for terrorism-related information. As a result of this guideline, the President issued a memorandum on May 9, 2008, regarding CUI. The CUI designation took the place of SBU designation for information. Currently, a CUI Council has been developed, and the CICC has appointed two representatives to sit on this council.

The FBI has expanded access to its Virtual Command Center capability. Intelink-U, RISS, and HSIN have announced the availability of this service to their user base, and LEO has demonstrated the ability to establish a virtual command center in near-real time.

The U.S. Department of Homeland Security (DHS) is also heavily engaged with the PM-ISE; state, local, and tribal public safety agencies; and the private sector to deploy a DHS Sensitive But Unclassified (SBU) Portal Interoperability Architecture based upon the newly reengineered Homeland Security Information Network (HSIN). Leveraging Service Oriented Architecture and GFIPM standards, DHS is building capabilities to link with RISSNET, LEO, and Intelink-U to create an interoperable, collaborative information sharing environment.

The Global Justice XML Data Model (GJXDM) is a standard that was designed specifically for criminal justice information exchanges. It provided the criminal justice community with a data standard to effectively share information. GJXDM standardized criminal justice information sharing for the first time and made it more economical and technically viable for agencies by offering standard tools, techniques, and data structures. GJXDM has fully evolved into the National Information Exchange Model (NIEM), where it exists as the "Justice" domain. NIEM has now extended information sharing capabilities into 15 other communities, or domains. The CICC has supported Global in the development

and release of NIEM and will continue to assist in the development of related guidance and resources, such as the integration of NIEM into the ISE-SAR Functional Standard.

Critical Element 9: Sustainability

The CICC, the Global Advisory Committee (GAC), DOJ, and DHS have partnered to identify and fund initiatives implementing the recommendations of the NCISP. The *Fusion Center Guidelines* was developed as a result of the NCISP, as were many other initiatives, including the:

- *Law Enforcement Analytic Standards*
- *Analyst Toolbox*
- *Minimum Criminal Intelligence Training Standards*
- *Baseline Capabilities for State and Major Urban Area Fusion Centers*
- *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*
- *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces*

Appendix D—CICC Membership

Chair

Bart R. Johnson
Executive Director, International Association of Chiefs of Police

Vice Chair

Vernon Keenan
Director, Georgia Bureau of Investigation
Association of State Criminal Investigative Agencies

Art Acevedo
Chief of Police, Austin, Texas, Police Department
Major Cities Chiefs Association

Richard Beary
Chief of Police, University of Central Florida
International Association of Chiefs of Police

Rodney G. Benson
Chief of Intelligence,
U.S. Drug Enforcement Administration

Ron Brooks
National Narcotics Officers' Associations' Coalition

James H. Davis
Executive Director, Colorado Department of Public Safety
National Governors Association

Michael Downing
Deputy Chief, Los Angeles, California, Police Department
Major Cities Chiefs Association

Joseph "Rick" Fuentes
Colonel, New Jersey State Police
International Association of Chiefs of Police

Doug Gillespie
Sheriff, Las Vegas, Nevada, Metropolitan Police Department
Major County Sheriffs' Association

Van Godsey
Assistant Director, Division of Drug and Crime Control, Missouri State Highway Patrol
Association of Law Enforcement Intelligence Units (LEIU)

Jenny Johnstone
President, International Association of Law Enforcement Intelligence Analysts

Donald Kennedy
Executive Director, New England State Police Information Network®
Regional Information Sharing Systems® Program

Marlon C. Lynch
Associate Vice President for Safety & Security, University of Chicago
International Association of Campus Law Enforcement Administrators

Scott MacGregor
Chief, California Highway Patrol

Mark Marshall
Sheriff, Isle of Wight County, Virginia, Sheriff's Office
National Sheriffs' Association

James McDermond
Assistant Director, Bureau of Alcohol, Tobacco, Firearms and Explosives

Peter Modafferi
Chief of Detectives, Rockland County, New York, District Attorney's Office
International Association of Chiefs of Police

Daniel Oates
Chief, Aurora, Colorado, Police Department

Kurt Schmid
Executive Director, Chicago, Illinois, High Intensity Drug Trafficking Area

Michael Sena
Deputy Director, Northern California Regional Intelligence Center
National Fusion Center Association

Kerry Sleeper
Deputy Assistant Director, Directorate of Intelligence
Federal Bureau of Investigation

Keith Squires
Commissioner, Utah Department of Public Safety
National Governors Association

Richard Stanek
Sheriff, Hennepin County, Minnesota, Sheriff's Office
Major County Sheriffs' Association

Craig Steckler
Chief, Fremont, California, Police Department
International Association of Chiefs of Police

Mark Wasylyshyn
Sheriff, Wood County, Ohio, Sheriff's Office
National Sheriffs' Association

The CICC also recognizes the following individuals as active partners in the Council's missions and objectives:

Scott McAllister
Deputy Under Secretary, State and Local Program Office, Office of Intelligence and Analysis, U.S. Department of Homeland Security

Kshemendra Paul
Program Manager, Information Sharing Environment

Russell Porter
Director of Federal, State, Local, and Tribal Partnerships, Office of the Director of National Intelligence

Appendix E—Glossary

Administrative Analysis—The provision of economic, geographic, or social information to administrators. (Gottlieb, Singh, and Arenberg, 1995, p. 13)

Analysis (law enforcement)—The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment. (Peterson, 1994, p. 269)

Collation—The process whereby information is stored and cross-referenced so that it can be retrieved easily. (INTERPOL, 1996, p. 10)

Collection—The directed, focused gathering of information from all available sources. (INTERPOL, 1996, p. 9)

Collection Plan—The preliminary step toward completing a strategic assessment that shows what needs to be collected, how it is going to be collected, and by what date. (Peterson, 1994, p. 36)

Confidential—Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Counterintelligence—Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, subversion, etc., that is related to national security concerns.

Crime Analysis—A set of systematic, analytical processes directed at providing timely and pertinent information relative to crime patterns and trend correlations to assist operational and administrative personnel in planning in the deployment of resources for the prevention and suppression of criminal activities, aiding the investigative process, and increasing apprehensions and the clearances of cases. (Gottlieb, Singh, and Arenberg, 1995, p. 13)

Crime Analyst—Crime analysts systematically study crime and disorder problems as well as other police-related issues—including sociodemographic, spatial, and temporal factors—to assist the police in criminal apprehension, crime and disorder reduction, crime prevention, and evaluation. (Boba, 2005)

Crime Pattern Analysis—Examining the nature, extent, and development of crime in a geographical area and within a certain period of time. (Europol, 2000, Insert 3)

Criminal Analysis—The application of analytical methods and products to data within the criminal justice field. (Peterson, 1994, p. 2)

Criminal Intelligence—Information compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Criminal Investigative Analysis—The use of components of a crime and/or the physical and psychological attributes of a criminal to ascertain the identity of the criminal. (Peterson, 1994, p. 42)

Data Element—A field within a database that describes or defines a specific characteristic or attribute.

Data Owner—An agency or an analyst that originally enters information or intelligence into a system.

Descriptive Analysis—Data and information systematically organized, analyzed, and presented. (Europol, 2000, Insert 3)

Dissemination—The release of information, usually under certain protocols. (Peterson, 1994, p. 271)

Evaluation—An assessment of the reliability of the source and accuracy of the raw data. (Morris and Frost, 1983, p. 4)

Explanatory Analysis—Analysis that attempts to understand the causes of criminality. It often includes the study of a large amount of variables and an understanding of how they are related to each other. (Europol, 2000, Insert 3)

Feedback/Reevaluation—Reviews the operation of the intelligence process and the value of the output to the consumer. (Harris, 1976, p. 133)

Forecasting—The process that predicts the future on the basis of past trends, current trends, and/or future speculation. (Peterson, 1994, p. 46)

Fusion Liaison Officer (FLO)—Fusion Liaison Officers act as a point of contact for their agency and typically are associated with information exchange between a fusion center and another agency (law enforcement or non-law enforcement) or partner. FLOs may focus on SAR information, terrorism-related information, or other major crimes.

Indicator—Detectable actions and publicly available information revealing critical information. (Krizan, 1999, p. 63)

Inference Development—Drawing conclusions based on facts. (Peterson, 1994, p. 48)

Information Classification—Protects sources, investigations, and the individual's right to privacy and includes levels: sensitive, confidential, restricted, and unclassified. (LEIU File Guidelines, as printed in *Intelligence 2000: Revising the Basic Elements*, 2001, p. 206)

Intelligence—The product of systematic gathering, evaluation, and synthesis of raw data on individuals or activities suspected of being or known to be criminal in nature. (Quoted in IACP, 1985, p. 5, from National Advisory Committee on Criminal Justice Standards and Goals, *Organized Crime,* 1976, p. 122) Intelligence is information that has been analyzed to determine its meaning and relevance. Information is compiled, analyzed, and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity. (IACP National Law Enforcement Policy Center, 1998)

Intelligence Analyst—Intelligence analysts utilize criminal intelligence information to create intelligence products that support decision making in the areas of law enforcement, crime reduction, and crime prevention. (Ratcliffe, Jerry H., Ph.D. *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders*, Second Edition)

Intelligence Cycle—Planning and direction, collection, processing and collating, analysis and production, dissemination. (Morehouse, 2001, p. 8)

Intelligence Files—Stored information on the activities and associations of individuals, organizations, businesses, and groups who are suspected of being or having been involved in the actual or attempted planning, organizing, financing, or commission of criminal acts or are suspected of being or having been involved in criminal activities with known or suspected crime figures. (LEIU Guidelines, in Peterson, Morehouse, and Wright, 2001, p. 202)

Intelligence-Led Policing—The collection and analysis of information to produce an intelligence end product designed to inform police decision making at both the tactical and strategic levels. (Smith, 1997, p. 1)

Intelligence Liaison Officer (ILO)—Intelligence Liaison Officers act as a point of contact for their agency and typically are associated with information exchange between their agency and another agency (law enforcement or non-law enforcement) or partner. ILOs may focus on SAR, terrorism, or other major crime information.

Investigative Information—Information obtained from a variety of sources—public, governmental, confidential, etc. The information may be utilized to further an investigation or could be derived from an investigation.

Need-to-Know—Indicates that an individual requesting access to criminal intelligence data has the need to obtain the data in order to execute official responsibilities.

Network—A structure or system of connecting components designed to function in a specific way.

Operational Analysis—Identifying salient features such as groups of or individual criminals, relevant premises, contact points, and methods of communication. (Europol, 2000, Insert 3)

Operational Intelligence—Intelligence that details patterns, modus operandi, and vulnerabilities of criminal organizations but is not tactical in nature. (Morris and Frost, 1983, p. vi)

Operations Analysis—The analytic study of police service delivery problems, undertaken to provide commanders and police managers with a scientific basis for a decision or action to improve operations or deployment of resources. (Gottlieb, Singh, and Arenberg, 1995, p. 34)

Pointer Index—A listing within a database containing particular items that serve to guide, point out, or otherwise provide a reference to more detailed information.

Predicate—The basis for the initiation of any inquiry or investigation.

Predictive Analysis—Using either descriptive or explanatory analytical results to reduce uncertainties and make an "educated guess." (Europol, 2000, Insert 3)

Preventive Intelligence—Product of proactive intelligence. (Morris and Frost, 1983, p. 6)

Privacy—An individual's interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include

privacy of personal behavior, privacy of personal communications, and privacy of personal data.

Proactive—Obtaining data regarding criminal conspiracies in order to anticipate problems and forestall the commission of crimes. (Morris and Frost, 1983, p. 6)

Problem Profile—Identifies established and emerging crime or incident series. (NCIS, 2001, p. 18)

Procedural Guidelines—Every criminal justice agency should establish procedural guidelines designed to provide a basic and general description for the collection of intelligence data. The guidelines should take into consideration the right of privacy and any other constitutional guarantees. (IACP, 1985, p. 6)

Reasonable Suspicion—When information exists that establishes sufficient fact to give a trained law enforcement 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. (Criminal Intelligence Systems Operating Policies, as printed in Peterson, Morehouse, and Wright, 2001, p. 212)

Recommendations—Suggestions for action to be taken by law enforcement management as a result of an analysis. (Peterson, 1994, p. 275)

Requirements—Validated and prioritized statements of consumers' needs for intelligence information. (Morris and Frost, 1983, p. vi)

Restricted Data—Reports, which at an earlier date were classified sensitive or confidential, with the need for high-level security no longer existing.

Right-to-Know—An individual requesting access to criminal intelligence data has the right to access due to legal authority to obtain the information pursuant to a court order, statute, or decisional law.

Risk Assessment—A report aimed at identifying and examining vulnerable areas of the society that are or could be exploited. (Europol, 2000, Insert 3) (*Also see Vulnerability Assessment.*)

Secret—Applied to information of which the unauthorized disclosure could reasonably be expected to cause serious damage to national security.

Security—A series of procedures and measures that, when combined, provide protection of people from harm, information from improper disclosure or alteration, and assets from theft or damage. (Criminal Justice Commission, 1995, as reprinted in *Intelligence 2000: Revising the Basic Elements*, p. 159)

Sensitive Data—Information pertaining to significant law enforcement cases currently under investigation and criminal intelligence reports that require strict dissemination and release criteria.

Situation Report—A mainly descriptive report that is oriented only towards the current crime situation. (Europol, 2000, Insert 3)

Social Media—Forms of electronic communication (such as Web sites used for social networking) through which users create online communities to share information, ideas, personal messages, and other content.

Strategic Assessment—A long-term, high-level look at the law enforcement issues that not only considers current activities but also tries to provide a forecast of likely developments. (NCIS, 2001, p. 17)

Strategic Intelligence—Most often related to the structure and movement of organized criminal elements, patterns of criminal activity, activities of criminal elements, projecting criminal trends, or projective planning. (IACP, 1985, p. 6, from National Advisory Committee and Criminal Justice Standards and Goals, *Organized Crime*, 1976, p. 122)

System—A group of databases that interact and form a whole structure.

Tactical Assessment—Ability to identify emerging patterns and trends requiring attention, including further analysis. (NCIS, 2000, p. 17)

Tactical Intelligence—Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety. (IACP, 1998, as reprinted in Peterson, Morehouse, and Wright, 2001, p. 218)

Target Profile—A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals. (NCIS, 2001, p. 18)

Tear-Line Report—A classified report that has information redacted from its content, primarily relating to the source of the data and method of collection.

Terrorism Liaison Officer (TLO)—Terrorism Liaison Officers act as a point of contact for their agency and typically are associated with information exchange between their agency and another agency (law enforcement or non-law enforcement) or partner. TLOs primarily focus on terrorism-related information.

Threat Assessment—A strategic document that looks at a group's propensity for violence or criminality or the possible occurrence of a criminal activity in a certain time or place. (Peterson, 1994, pp. 56–57)

Top Secret—Applied to information of which the unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

Unclassified Data—Civic-related information to which, in its original form, the general public had direct access (i.e., birth and death certificates). This would also include newspaper, magazine, and periodical clippings.

Vet—To subject to an expert appraisal or examine and evaluate for correctness.

Vulnerability Assessment—A strategic document that views the weaknesses in a system that might be exploited by a criminal endeavor.

Warning—A tactical warning is a very short-term warning that attack is either under way or so imminent that the forces are in motion or cannot be called back. A strategic warning is any type of warning or judgment issued early enough to permit decision makers to undertake countermeasures—ideally such warning may enable (them) to take measures to forestall the threat altogether. (Grabo, 1987, p. 6)

Appendix F—Acronyms

ADNET-U	Anti-Drug Network-Unclassified
AES	Advanced Encryption Standard
ARJIS	Automated Regional Justice Information System
ATIX	Automated Trusted Information Exchange
BJA	Bureau of Justice Assistance
CATIC	California Anti-Terrorism Information Center
CDICG	Counterdrug Intelligence Coordinating Group
CDX	Counterdrug Intelligence Executive Secretariat
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordinating Council
CIO	Chief Information Officer
CISAnet	Criminal Information Sharing Alliance Network
CJIS	Criminal Justice Information Services
CLEAR	Chicago Citizen and Law Enforcement Analysis and Reporting
COP	Community Oriented Policing
CUI	Controlled Unclassified Information
DEA	U.S. Drug Enforcement Administration
DES	Data Encryption Standard
DHS	U.S. Department of Homeland Security
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence
DoD	U.S. Department of Defense
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
FBI	Federal Bureau of Investigation
FLO	Fusion Liaison Officer
FOUO	"For Official Use Only" information handling caveat
GAC	Global Justice Information Sharing Initiative Advisory Committee
GFIPM	Global Federated Identity and Privilege Management
GISWG	Global Justice Information Sharing Initiative Infrastructure/Standards Working Group
GIWG	Global Justice Information Sharing Initiative Intelligence Working Group
Global	Global Justice Information Sharing Initiative
GRA	Global Reference Architecture
GSC	Global Standards Council
GSWG	Global Justice Information Sharing Initiative Security Working Group
HIDTA	High Intensity Drug Trafficking Areas
HSIN	Homeland Security Information Network
HS SLIC	Homeland Security State & Local Intelligence Community of Interest
IACP	International Association of Chiefs of Police
IADLEST	International Association of Directors of Law Enforcement Standards and Training
IAFIS	Integrated Automated Fingerprint Identification System
IALEIA	International Association of Law Enforcement Intelligence Analysts
III	Interstate Identification Index
ILO	Intelligence Liaison Officer

ISE	Information Sharing Environment
ISI	Gateway Information Sharing Initiative
IT	Information Technology
JCON	Justice Consolidated Office Network
JITF-CT	Joint Intelligence Task Force-Combating Terrorism
JRIES	Joint Regional Information Exchange System
JTTF	Joint Terrorism Task Force
LEADS	Law Enforcement Agencies Data System
LEIN	Law Enforcement Intelligence Network
LEIU	Association of Law Enforcement Intelligence Units
LEO	Law Enforcement Online
LES	"Law Enforcement Sensitive" information-handling caveat
MATRIX	Multistate Anti-Terrorism Information Exchange
NAS	National Alert System
NCIC	National Crime Information Center
NCISP	*National Criminal Intelligence Sharing Plan*
N-DEx	Law Enforcement National Data Exchange
NDIC	National Drug Intelligence Center
NDPIX	National Drug Pointer Index
NFCA	National Fusion Center Association
NICS	National Instant Criminal Background Check System
NIEM	National Information Exchange Model
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
Nlets	Nlets, The International Justice and Public Safety Network
NSA	National Sheriffs' Association
NSI	Nationwide SAR Initiative
NSIS	*National Strategy for Information Sharing*
NSISS	*National Strategy for Information Sharing and Safeguarding*
NTAS	National Terrorism Advisory System
NW3C	National White Collar Crime Center
NYPD CTB	New York Police Department Counterterrorism Bureau
OJP	Office of Justice Programs
OSIS	Open Source Information System
PM-ISE	Program Manager for the Information Sharing Environment
PMO	Program Management Office
RISS	Regional Information Sharing Systems
RISSNET	Regional Information Sharing Systems Secure Cloud
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
SIG	Special Interest Group
SPPADS	State and Provincial Police Academy Directors Section
TLO	Terrorism Liaison Officer
TSA	Transportation Security Administration
UCR	Uniform Crime Reporting
VPN	Virtual Private Network
W3	World Wide Web Consortium
XML	Extensible Markup Language