COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
POLICE
SINCE 1893

PMASE.

U.S. DEPARTMENT OF HOMELAND SECURITY

NATIONAL SUMMIT ON INTELLIGENCE

GATHERING, SHARING, ANALYSIS, AND USE AFTER 9-11

MEASURING SUCCESS AND SETTING GOALS FOR THE FUTURE

September 2008

International Association of Chiefs of Police

Dear Colleague:

I am very pleased to provide you with the final report of our *National Summit on Intelligence Sharing: Gathering, Sharing, Analysis and Use After 9-11: Measuring Success and Setting Goals for the Future.* This summit was a follow up to our original 2002 intelligence summit, and it focused on both progress made since the terrorist attacks of 2001, and the work remaining to be accomplished.

You'll note from the letter on the next page that we were fortunate to have the strong support of several Federal partners—the Office of Community Oriented Policing Services (COPS), the Department of Homeland Security (DHS) and the Program Manager, Information Sharing Environment (PM-ISE) in the Office of the Director of National Intelligence. We are grateful for their desire to address the future of national intelligence with us collaboratively.

As you read this report, I hope you'll find that it fairly and accurately represents the accomplishments achieved since 2002, as well as the obstacles that remain. Most importantly, I hope that you will see the value in the eight strategic recommendations that emerged from the summit. We believe that these recommendations, once implemented, will move us forward in rapid fashion to improve law enforcement's capacity to gather, analyze, share and use intelligence to prevent crimes of all types and to protect our citizens.

Finally, I want to make it clear that the findings from the summit come from the diligent and thoughtful work of the 150 law enforcement and other experts who joined us last November at the summit. This is their product, and as President of the IACP, I'm proud to present it to the nation.

Sincerely,

Ronald C. Ruecker
Director of Public Safety
Sherwood, Oregon
IACP President

Dear Colleague:

In the seven years since our nation withstood devastating terrorist attacks here at home, the role of law enforcement has become recognized as vital to the Nation's safety and security. Once again, the law enforcement community has risen to this challenge. Information exchange between local, state, tribal, and federal law enforcement and homeland security partners has improved tremendously, thanks to advances in technology, improved partnership between federal, state and local authorities and greater trust among ourselves and the communities we serve.

In 2002, the Office of Community Oriented Policing Services (COPS), in partnership with the International Association of Chiefs of Police (IACP), hosted a Criminal Intelligence Sharing Summit that resulted in the National Criminal Intelligence Sharing Plan, the establishment of the Global Intelligence Working Group, and the Criminal Intelligence Coordinating Council, the latter of which advises the U.S. Attorney General on justice information sharing and integration initiatives.

Five years later, in November of 2007, the COPS Office and IACP held the *Criminal Intelligence Sharing Summit: Measuring Success and Setting Goals for the Future.* The U.S. Department of Homeland Security and the Office of the Program Manager for the Information Sharing Environment joined the partnership and co-sponsored this event. Both these agencies were created since the first summit was held, demonstrating the breadth of change that has occurred in the ensuing years.

This last Summit convened more than 150 state, local, tribal, and federal law enforcement and public safety leaders, intelligence analysts, and academics to discuss what next steps were needed to improve information sharing. Discussion at this summit centered on raising awareness about the Information Sharing Environment, fusion centers, and intelligence-led policing. The key to the success of these efforts falls under the community policing umbrella – problem solving, partnerships, and organizational transformation. This report includes eight significant recommendations on how the law enforcement community can continue to work together to ensure that hometown security is homeland security. We look forward to working together with you to implement these recommendations.

Sincerely,

Carl R. Peed, Director
Office of Community Oriented Policing Services
Department of Justice

Thomas E. McNamara, Program Manager
Information Sharing Environment
Office of the Director of National Intelligence

Robert C. Riegle, Director
State and Local Program Office
Department of Homeland Security

CONTENTS

ACKNOWLEDGMENTS

EXECUTIVE SUMMARY

Criminal intelligence sharing in the United States has come a long way since March 2002, the date of the first summit on criminal intelligence sharing, co-sponsored by the International Association of Chiefs of Police (IACP) and the U.S. Department of Justice Office of Community Oriented Policing Services. That summit resulted in the *National Criminal Intelligence Sharing Plan* and a council of law enforcement executives—the Criminal Intelligence Coordinating Council—to oversee its implementation. There were other achievements, too. The Global Justice Information Sharing Initiative produced dozens of products to help law enforcement agencies share information and intelligence. Fusion centers and Joint Terrorism Task Forces fostered new levels of communication and collaboration across jurisdictions. The Federal Government created the Department of Homeland Security, the Office of the Director of National Intelligence, and the Office of the Program Manager for the Information Sharing Environment.

The participants in the follow-up 2007 IACP Criminal Intelligence Sharing Summit nevertheless made it clear that many of the nation's law enforcement agencies do not participate in the criminal intelligence sharing plan. Too many state, local, and tribal agencies, it would seem, underestimate their importance to the criminal intelligence sharing process, overestimate the burdens of full participation, and/or remain unaware of how to contribute to the vital work of the plan.

The participants in the most recent summit reaffirmed their commitment to overcoming these challenges and helping law enforcement agencies of all sizes to participate more fully in the criminal intelligence sharing process. Together, they crafted a set of recommendations to help law enforcement agencies share information and intelligence seamlessly, while protecting privacy and civil rights.

What Is Criminal Intelligence Sharing?

Criminal intelligence sharing is the exchange of an analytical product designed to help police prevent, respond to, investigate, and solve crimes. The analytical product is the result of the intelligence process which includes the following steps: planning/direction, information collection, analysis, production, and finally feedback. Often times it is produced by an analyst who reviews the data and looks for crime trends, statements from informants and witnesses, observations by police officers, and other patterns. The analyst would then reach conclusions about likely criminal activity, summarize those conclusions in a forecast, and submit the forecast to law enforcement managers who can then consider the forecast before making decisions about strategies and tactics.

Criminal intelligence, it should be noted, is distinct from National Intelligence.[1] The goal of the National Intelligence effort is to provide the President, and the National Security Council, and the Homeland Security Council the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats.[2] The National Intelligence effort is led by the Director of National Intelligence, and conducted by the 16 federal agencies comprising the Intelligence Community, including the Central Intelligence Agency, the National Security Agency, and the National Geospatial Intelligence Agency.

Recent cases like that of the Lackawanna Six in New York, are examples of how local law enforcement, through the effective use of criminal intelligence, plays a vital role in detecting terrorist threats and protecting national security. The vigilance of officers who observe suspicious activity and notify the appropriate federal authorities is the key to terrorism prevention and homeland security. According to the *National Strategy for Information Sharing* issued by the White House in October 2007, "State, local, and tribal governments carry out their counterterrorism responsibilities within the broader context of their core mission to protect the public's health, safety, and to provide emergency and non-emergency services."[3]

Recommendations of the 2007 Criminal Intelligence Sharing Summit

To help law enforcement move closer to the vision of criminal intelligence sharing described in the *National Criminal Intelligence Sharing Plan,* the participants in the 2007 *Criminal Intelligence Sharing Summit: Measuring Success and Setting Goals for the Future* offer the following recommendations:

1.   Every state, local, and tribal law enforcement agency in the United States should strive to develop and maintain a criminal intelligence capability consisting of at least the following requirements: formal criminal intelligence awareness training for at least one sworn officer; training all levels of law enforcement personnel to recognize behavior

---

[1] National Intelligence is defined by the Section 3 of the National Security Act of 1947, as amended, as A) "information relating to the capabilities intentions or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" (known as foreign intelligence); and B) "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities (known as "counterintelligence"), regardless of the source from which derived and including information gathered within or outside the United States, that (A) pertains to more than one United States Government agency; and (B) involves (i) threats to the United States, its people, property, or interests'; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on the Untied States national or homeland security." (50 U.S.C. § 401a)
[2] Executive Order 12333, as amended
[3] The White House, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (Washington, D.C.: U.S. Government Printing Office, October 2007), 17, http://www.whitehouse.gov/nsc/infosharing/index.html.

indicative of criminal activity associated with terrorism; and defined procedures and mechanisms for communication with the nearest fusion center and/or a regional information sharing network.

2.   A nationwide marketing and training initiative should be designed to convince every law enforcement agency to participate in criminal intelligence sharing, make every law enforcement agency aware of the criminal intelligence resources available to it, and give every law enforcement agency the know-how to participate in criminal intelligence sharing.

3.   All law enforcement organizations and agencies should explore potential partnerships in order to enhance analytical capacity within their agencies.

4.   Chief executives of state, local, and tribal law enforcement agencies should encourage the directors of all criminal intelligence sharing initiatives and resources (such as fusion centers) to adopt and maintain an all-crimes approach.

5.   Fusion center directors and their law enforcement partners should take a series of steps to improve the effectiveness of the centers, including forming an association of fusion centers that might help promote the sharing of best practices among fusion centers and help promote the work of the centers to law enforcement agencies and policymakers at all levels.

6.   The U.S. Department of Homeland Security, the Office of the Director of National Intelligence, and the U.S. Department of Justice should work together to simplify and streamline security classifications and clearances.

7.   Policymakers at the federal, state, local, and tribal levels should continue to take steps to enhance the protection of privacy, civil liberties, and civil rights and ensure that communities are aware of, and engaged in, the process.

8.   Law enforcement executives should develop ways to measure the success of criminal intelligence sharing and recognize those individuals involved in that success.

INTRODUCTION

Criminal Intelligence Sharing and Community Oriented Policing

On the morning of December 14, 2007 two men pleaded guilty to federal terrorism charges in a U.S. District Court in California; a third man pleaded guilty three days later. Prosecutors described the three men as U.S. citizens who formed a radical Islamic terrorist cell while in prison and then prepared the attacks after their release. They admitted to conspiring to attack U.S. military installations, Israeli government offices, and synagogues in Los Angeles.

Who uncovered the plot? It was not covert operatives in Afghanistan or federal agents conducting an investigation on suspected Al Qaeda members. It was local police officers investigating a gas station robbery in Torrance, a Los Angeles suburb. They found papers containing details of the terrorist plot while searching the apartment where two robbery suspects lived. The Torrance Police Department shared the information with other agencies, including the Federal Bureau of Investigation (FBI). The ensuing investigation involved 300 local, state, and federal police officers.

Officials say police arrested the men for robbery about two months before they intended to launch the attacks. Cell members had already purchased weapons for the attacks with the money they had stolen during a string of gas station holdups.

The Torrance case reminds us that good police work can help prevent acts of terrorism. As Ambassador Thomas "Ted" McNamara, Program Manager for the Information Sharing Environment (PM-ISE), said at the 2007 Criminal Intelligence Sharing Summit, "State and local authorities carry out efforts to combat terrorism as part of their core mission of protecting local communities from crime, violence, and disorder." The Torrance case also reminds us that it is not only big-city police officers who should be on the lookout for signs of terrorist activity; terrorists live in communities of all kinds, including quiet suburbs like Torrance, while they plan their attacks and even commit the crimes that are forerunners of those attacks.

U.S. law enforcement agencies have made progress as sharers of information and intelligence since September 11, 2001. Officers are more aware that they could find evidence of terrorist plans and encounter would-be terrorists while carrying out their normal police duties. Police agencies, especially in metropolitan areas, are better prepared to develop, manage, and share intelligence and to work together to disrupt terrorist plots. The Federal Government, for its part, has enacted laws, adopted regulations, and created systems and procedures designed to facilitate information and intelligence sharing by police departments and other public safety and homeland security agencies at all levels.

In spite of the progress made in recent years, the intelligence process itself remains a mystery to many police officers, and some law enforcement executives consider their agencies too small or too remote to participate in criminal intelligence sharing. According to 2007 summit participants, however, every law enforcement agency has a job to do in criminal intelligence sharing.

Criminal intelligence is "the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."[4]   The criminal intelligence process, according to the *National Criminal Intelligence Sharing Plan*, consists of six steps:

1. Planning the gathering of information
2. Gathering the information
3. Processing the information
4. Analyzing the information to produce an intelligence product
5. Disseminating the intelligence product to someone who needs it, can use it, and has a right to it
6. Evaluating the usefulness of the intelligence product

Information, as it is understood here, can be any kind of data—a license plate number, a criminal record, an officer's observation of a particular person's presence at a particular place at a particular time, or an item gleaned from a newspaper article. Processing the information includes verifying that it satisfies legal requirements of relevance to a criminal investigation. Analysis involves synthesizing, evaluating, and contextualizing the information, drawing conclusions from the information, and expressing those conclusions in an intelligence product, such as a report, an estimate, or a forecast.

Levels of Intelligence

Intelligence-Led Policing: The New Intelligence Architecture, produced by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, classifies U.S law enforcement agencies according to the level of their intelligence capability:

Intelligence Level 1
• Employs an intelligence manager, intelligence officers, and professional intelligence analysts
• Produces intelligence products for its own use and routinely shares intelligence products with other agencies
• Is typically a national or large state agency with hundreds or thousands of sworn officers (such as the National Drug Intelligence Center, the Financial Crimes Enforcement Network, and the California Department of Justice)

Intelligence Level 2
• Employs an intelligence manager, intelligence officers, and professional intelligence analysts
• Produces tactical or strategic intelligence for its own use but does not have resources devoted to sharing intelligence
• Uses intelligence analysis to advance investigations into complex crimes such as insurance fraud
• Is typically a state police department or a large municipal or county law enforcement agency with hundreds or thousands of sworn officers

continued

---

[4] U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies,* by David L. Carter (Washington, D.C.: U.S. Government Printing Office, November 2004), 9.

Naturally, not every police department has the need or the resources to carry out all six steps of the criminal intelligence process. But every law enforcement agency can and should develop criminal intelligence capability at a level that is appropriate for its size and mission.[5] All agencies, even the smallest, should strive to achieve at least minimal criminal intelligence capabilities: formal criminal intelligence awareness training for at least one sworn officer; training all levels of law enforcement personnel to recognize behavior indicative of criminal activity associated with terrorism; and defined procedures and mechanisms for communication with the nearest fusion center and/or a regional information sharing network.

Lastly, law enforcement officials must bear in mind the importance of cultivating community partnerships as part of their efforts to develop and share criminal intelligence. In his remarks at the 2007 summit, Carl Peed, Director of the U.S. Department of Justice Office of Community Oriented Policing Services (COPS), emphasized the close connection between intelligence-led policing (ILP) and community policing: "ILP can take advantage of the partnerships built through community policing by leveraging the trust between citizens and law enforcement; ILP can be informed by the problem-solving process [at the core of community policing]; and it can also benefit from the organizational transformation inherent in community policing. Put simply, ILP is not just consistent with community policing, but it fits well under the community policing umbrella."

Intelligence Level 3
• Employs intelligence officers who typically have received some training in intelligence capability but does not employ professional analysts
• May develop intelligence products for internal use but typically relies on level 1 intelligence agencies for intelligence products
• Typically a local, state, or tribal law enforcement agency with dozens or hundreds of sworn officers

Intelligence Level 4
• Employs no intelligence officers or analysts but may assign part-time intelligence capability duties to an officer
• Has obtained intelligence training for one or more officers
• Participates in regional information sharing networks
• Has a few dozen sworn officers at most but, like the majority of U.S. law enforcement agencies, probably has fewer

Source: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Intelligence-Led Policing: A New Architecture*, in the series *New Realities: Law Enforcement in the Post–9/11 Era*, by IACP with the National Sheriffs Association, Major Cities Chiefs Association, Police Foundation, and NOBLE (Washington, D.C.: U.S. Government Printing Office, 2005), 12–13.

---

[5] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Intelligence-Led Policing: A New Architecture,* in the series *New Realities: Law Enforcement in the Post–9/11 Era*, by IACP with the National Sheriffs Association, Major Cities Chiefs Association, Police Foundation, and NOBLE (Washington, D.C.: U.S. Government Printing Office, 2005), 13.

SUMMIT BACKGROUND

Since 1994, the International Association of Chiefs of Police (IACP) has convened more than a dozen national policy summits on matters of concern to law enforcement executives and their peers in related disciplines. Topics have included DNA evidence, hate crime, safety in Indian country, family violence, youth violence, child protection, and many others.

In March 2002, law enforcement leaders and intelligence experts gathered in Alexandria, Virginia, at the IACP Criminal Intelligence Sharing Summit. Participants sought ways to help police share information and intelligence with a single goal in mind: preventing another terrorist attack like the one that had occurred just six months earlier. They drafted the following expression of purpose to guide their work:

> *The United States law enforcement community is universally committed to the timely and seamless exchange of terrorist and criminal information and intelligence. In light of the tragedy of September 11, it is absolutely critical that all law enforcement personnel work together to protect the nation, and we are committed to doing so.*

Their work produced an influential set of recommendations:

- Create a national intelligence plan
- Create a criminal intelligence coordinating council
- Adopt intelligence-led policing
- Protect civil rights
- Increase opportunities for building trust among police agencies
- Fix deficits in analytic capacity and information sharing capacity
- Improve criminal intelligence training
- Improve criminal intelligence technology

Five years later, the IACP and its partners including the COPS Office, PM-ISE, and the Department of Homeland Security (DHS), convened another summit to determine the state of criminal intelligence sharing. Police leaders from agencies of various kinds (including federal, state, local, tribal, and campus) and sizes joined federal policy makers, intelligence experts, and others in Washington, D.C., to consider how successfully the nation's 18,000 law enforcement agencies have carried out the recommendations from the 2002 summit. What have they accomplished in the last five years? What new problems and solutions have they discovered? What should they do next?

The summit provided an opportunity to identify obstacles and concerns, find solutions, and create an action plan to engage all state, county, local, and tribal police agencies in intelligence gathering, analysis, and sharing. Participants focused on the following areas in small breakout groups: fusion centers; intelligence-led policing; privacy and civil liberties; training and technical assistance; building an analytical capacity; and sharing classified and unclassified information.

At the 2007 summit, Ron Ruecker, president of the IACP and director of public safety in Sherwood, Oregon, challenged participants to make the second summit "bigger, bolder, and much broader in scope" than the 2002 event. He asked them to be candid with one another as they identified obstacles to criminal intelligence sharing and to help develop ways to overcome those obstacles.

ACCOMPLISHMENTS SINCE 2002

A number of key recommendations from the 2002 IACP summit on criminal intelligence have produced meaningful results. What follows is a summary of selected achievements of criminal intelligence stakeholders in the years since the summit.

Create a national intelligence plan

The 2002 summit called for the creation of a national intelligence plan that recognized the need for sharing both criminal intelligence and national intelligence between and among police agencies at all levels. The summit participants understood that even while on heightened alert for terrorist activity, local, state, and tribal police departments would need to carry out their mission of detecting, preventing, and investigating crimes. They were also aware that police officers had found evidence of terrorist activities and apprehended terrorists during the course of their normal duties. Enhancing criminal intelligence sharing could only improve the chances that a police officer might uncover a threat to homeland security while conducting a criminal investigation, enforcing traffic laws, or carrying out community policing responsibilities.

As a direct result of the summit recommendation, the U.S. Department of Justice (DOJ) issued the *National Criminal Intelligence Sharing Plan* (NCISP) in October 2003. In it, the plan's developers, the Global Intelligence Working Group (GIWG), made 28 recommendations designed to bring about "a nationwide communications capability that will link together all levels of law enforcement personnel, including officers on the streets, intelligence analysts, unit commanders, and police executives for the purpose of sharing critical data."

The plan proved to be the first in a series of refinements of a national strategy for intelligence sharing. The following year, President George W. Bush signed into law the Intelligence Reform and Terrorism Prevention Act of 2004. Among other provisions, the law established the Office of the Director of National Intelligence (DNI) and the Office of the Program Manager for the Information Sharing Environment (PM-ISE), which released the *Information Sharing Environment Implementation Plan* in November 2006.

In 2005, DHS, DOJ, and the Global Justice Information Sharing Initiative (Global) released *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era.*

Most recently, in October 2007 the White House issued the *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing,* which calls for a national information sharing capability through the establishment of a national integrated network of fusion centers. Since 2001, the federal government has provided significant grant funding, training, and technical assistance to support the establishment of fusion centers operated by states and major urban areas. The Strategy builds on these efforts and provides a federal government-wide approach to interfacing and collaborating with these fusion centers. Additionally, Appendix I of the Strategy outlines the federal, state, local, and tribal governments' roles and responsibilities for the establishment and continued operations of state and major urban area fusion centers.

Create a criminal intelligence coordinating council

The Criminal Intelligence Coordinating Council (CICC) formed in 2004 to provide recommendations in connection with the implementation and refinement of the NCISP. Global, of which the CICC is a part, advises the U.S. Attorney General on justice information sharing and integration initiatives and supports the exchange of pertinent justice and public safety information. It promotes standards-based electronic information exchange to provide the justice community with timely, accurate, complete, and accessible information in a secure and trusted environment. The CICC and its research partner the GIWG serve as advocates for local law enforcement in their efforts to develop and share criminal intelligence for the promotion of public safety and the security of our nation.

The council comprises 20 law enforcement executives, intelligence analysts, and federal policymakers. Among other achievements, the CICC has helped create minimum training standards for intelligence analysts, police officers, and others. Those training standards were updated in 2007.[6]

Adopt intelligence-led policing

The phrase *intelligence-led policing* enjoys wide currency among criminal justice researchers and national policymakers. There is vigorous debate among them about what exactly intelligence-led policing is, but most agree that it integrates easily with other popular policing models, including community policing, problem-oriented policing, and

---

[6] U.S. Department of Justice, Global Justice Information Sharing Initiative, Counterterrorism Training Coordination Working Group, *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States: Findings and Recommendations* (October 2007), http://it.ojp.gov/documents/min_crim_intel_stand.pdf.

CompStat. *Law Enforcement Intelligence*, a 2004 COPS Office publication, describes intelligence-led policing as "the integration of community policing and law enforcement intelligence."[7] The report *Intelligence-Led Policing: The New Intelligence Architecture,* issued by the Bureau of Justice Assistance (BJA) and their partners in 2005, calls it "a collaborative enterprise based on improved intelligence operations and community oriented policing and problem solving."[8]

Stakeholders have taken measures to encourage law enforcement agencies to embrace intelligence-led policing or at least make criminal intelligence sharing a point of emphasis. Global, for instance, produced a one-page resource document designed to inspire police executives to take 10 simple steps to become participants in developing and sharing criminal intelligence.

Protect privacy, civil liberties, and civil rights

Police leaders at all levels have acknowledged the importance of protecting privacy, civil liberties, and civil rights in any intelligence-sharing initiative. A body of literature on the subject has emerged to guide practitioners. Global, for instance, published both *The Privacy Policy Development Guide*[9] in 2006 and *Privacy, Civil Rights, and Civil Liberties: Policy Templates for Justice Information* in 2008.[10] Additionally In September 2006, the IACP published *Protecting Civil Rights: A Leadership Guide for State, Local, and Tribal Law Enforcement.*

In addition, the joint DHS/DOJ Fusion Process Technical Assistance Program has developed and is delivering the Fusion Center Privacy Policy Development Service. The service enables the development of an effective privacy policy to ensure that constitutional rights, civil liberties, and civil rights are protected while allowing the fusion center

---

> **10 Simple Steps to Help Your Agency Become a Part of the** *National Criminal Intelligence Sharing Plan*
>
> **1.** Recognize your responsibilities and lead by example. Recognize the value of sharing intelligence information within your own agency, and encourage the practice of sharing information with other law enforcement and public safety agencies. Use the guidelines and action steps outlined in the *National Criminal Intelligence Sharing Plan* ("Plan") to implement or enhance your organization's intelligence function.
>
> **2.** Establish a mission statement and a policy to address developing and sharing information and intelligence data within your agency.
>
> *continued*

---

[7] U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies,* by David L. Carter (Washington, D.C.: U.S. Government Printing Office, November 2004), 39.

[8] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Intelligence-Led Policing: A New Architecture*, in the series *New Realities: Law Enforcement in the Post–9/11 Era,* by IACP with the National Sheriffs Association, Major Cities Chiefs Association, Police Foundation, and NOBLE (Washington, D.C.: U.S. Government Printing Office, 2005), 13.

[9] U.S. Department of Justice, Global Justice Information Sharing Initiative, *Privacy Policy Development Guide* (October 2006), http://www.search.org/files/pdf/Privacy_Guide_Final.pdf.

[10] U.S. Department of Justice, Global Justice Information Sharing Initiative, *Privacy, Civil Rights, and Civil Liberties: Policy Templates for Justice Information* (February 2008), http://it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf.

to achieve its mission objectives. The President's National Strategy for Information Sharing identifies the administration's core privacy principles.

Increase opportunities for building trust among police agencies

The 2002 summit participants tasked the CICC with improving institutional trust among police agencies to encourage the sharing of information and intelligence, and they suggested two avenues for doing so: improving the security of shared information and emphasizing the importance of smaller, regional networks for information sharing. Global has attempted to address the security of information sharing systems by developing, publishing, and disseminating a guide called *Applying Security Practices to Justice Information Sharing* in 2004. Trust building through regional networks is evolving through traditional RISS networks and contemporary fusion centers. Long-standing RISS networks continue to be conduits for the exchange of criminal intelligence among participating agencies. Participants in the 2007 summit suggested that other smaller, regional information networks are forming around the country without a great deal of intervention from national agencies.

Another significant development in the area of trust building is the establishment of fusion centers. *Fusion Center Guidelines* issued by Global recognize that "fostering a collaborative environment builds trust among participating entities [and] strengthens partnerships . . . ."[11] State and local governments have established over 60 fusion centers, and the Federal Government is committed to supporting the establishment of an integrated network of fusion centers to enhance our nation's information sharing capability. The *National Strategy for Information Sharing* designates fusion centers as the focus within the state and local environment for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism.

The Plan provides model policies and guidelines for implementing or reviewing an agency's intelligence function. Examples include Criminal Intelligence Systems Operating Policies federal regulation 28 CFR Part 23, the International Association of Chiefs of Police's Criminal Intelligence Model Policy, and the Law Enforcement Intelligence Unit's (LEIU) Criminal Intelligence File Guidelines.

3. Connect to your state criminal justice network and regional intelligence databases, and participate in information sharing initiatives. Many states provide access to other government databases, including motor vehicles, corrections, and others. Regional intelligence databases and sharing initiatives promote communication and collaboration by providing access to other agencies' and organizations' investigative and intelligence data.

4. Ensure privacy issues are protected in policy and practice. The protection of individuals' privacy and constitutional rights is an obligation of government officials and is crucial to the long-term success of criminal intelligence sharing. The Plan provides guidelines that support policies which will protect privacy and constitutional rights while not hindering the intelligence process. Implementing and supporting privacy policies and practices within your agency will also reduce your organization's liability concerns.

continued

---

[11] U.S. Department of Justice, Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era,* Guideline 4, Page 29 *(August 2005).*

The last six years saw a proliferation of interagency partnerships of other kinds, and these partnerships appear to represent opportunities for building trust among police agencies. The FBI and its law enforcement partners, for instance, have created more than 100 Joint Terrorism Task Forces (JTTFs).[12]

Remedy deficits in analysis capability

The 2002 summit charged the CICC with establishing analytical standards. Since then, Global and IALEIA published *Law Enforcement Analytic Standards* in 2004. Global issued *Law Enforcement Analyst Certification* Standards in 2006.[13] Global and its partners issued *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* in 2004 and updated the standards to reflect the current Information Sharing Environment in 2007. IALEIA also has built a basic level certification around the NCISP objectives for analysts with the Foundations of Intelligence Analysis Training.

Improve training

The 2002 summit recommendations emphasized the need to train both current and incoming officers on criminal intelligence sharing. In that spirit, the Global publication referenced earlier again serves as a useful guide *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* and updated them in 2007. The Intelligence Training Coordination Working Group and the Counterterrorism Training Coordination Working Group launched the Criminal Intelligence Training Master Calendar[14] in 2007.

5. Access law enforcement Web sites, subscribe to law enforcement listservs, and use the Internet as an information resource. Many Web sites on the Internet and others on closed networks provide valuable intelligence assessments and news. Listservs provide instant and widespread communication for investigators. Listservs allow both the receipt and distribution of intelligence information. The Internet provides a wealth of open-source information, including government information and access to private agencies that share with law enforcement.

6. Provide your agency members with appropriate training on the criminal intelligence process. Some training models or modules are already found in Internet-based and interactive CDs, such as the International Association of Law Enforcement Intelligence Analysts (IALEIA), National White Collar Crime Center, and LEIU "Turn Key Intelligence." A listing of available intelligence training sources and specifically scheduled classes is found on the IALEIA Web site: www.ialeia.org. This listing allows individuals to directly contact training source agencies and organizations for more information on classes and schedules.

continued

Developing and Sharing Information and Intelligence in a New Era, Guideline 4, Page 29 *(August 2005).*

[12] U.S. Department of Justice, Federal Bureau of Investigation, "Protecting America against Terrorist Attack: A Closer Look at the FBI's Joint Terrorism Task Forces," FBI Web site, December 1, 2004, http://www.fbi.gov/page2/dec04/jttf120114.htm.

[13] U.S. Department of Justice, Global Justice Information Sharing Initiative, *Law Enforcement Analyst Certification Standards* (August 2006), http://www.iir.com/global/products/law_enforcement_analyst_certification_standards.pdf.

[14] http://mastercalendar.ncirc.gov/

Improve technology

Participants in the 2002 summit cautioned that technological improvements could enhance criminal intelligence sharing capabilities only where good policies, careful training, and trust already existed. They also acknowledged that technology in 2002 was inadequate to the task at hand. Since then, Global has developed a markup language and dictionary designed to standardize data records and allow police agencies to share information seamlessly. The trend toward mobile computing has increased the number of police officers who can submit and retrieve information and intelligence files using computers in police vehicles. Technology has also enabled the enhanced protection of information privacy and civil liberties through automated procedures for redress, data quality, data security, notice mechanisms, and accountability, enforcement, and audit mechanisms. DOJ and DHS jointly developed the National Information Exchange Model, one of many efforts to improve the way agencies share information electronically. For more information on these efforts, readers may want to refer to the Epilogue in this report.

Source: U.S. Department of Justice, Bureau of Justice Assistance, Global Justice Information Sharing Initiative, "10 Simple Steps," revised August 2005, http://www.iir.com/global/products/Ten_steps.pdf

7. Become a member of your in-region Regional Information Sharing Systems (RISS) center. RISS operates the only secure Web-based nationwide network for communication and exchange of criminal intelligence information by local, state, federal, and tribal participating law enforcement member agencies. RISS partners with other law enforcement systems to electronically connect them to RISSNET, including High Intensity Drug Trafficking Areas (HIDTA) Investigative Support centers and other federal and state agency systems.

8. Become a member of the FBI's Law Enforcement Online (LEO) system. The FBI's LEO system is a sensitive but unclassified, real-time information sharing communications system for all levels of the law enforcement community and is available at no cost to its users. LEO provides secure e-mail capability, a national alert mechanism, and access to over 125 special-interest groups for sharing information by providing access to other networks, systems, databases, and other services.

9. Partner with public and private infrastructure sectors.
Regular communication with the entities that control America's critical infrastructures such as energy, agriculture, transportation, and shipping is critically important to ensuring the safety and security of the citizens in your community.

10. Participate in local, state, and national intelligence organizations. In most areas of the country, there are locally based intelligence organizations that welcome participation from all agencies and are often affiliated with state and national organizations.

14

CHALLENGES NOT YET OVERCOME

For all the advances since 2002, some barriers are preventing or slowing progress on the recommendations from the first summit. The following is a list of selected obstacles identified by participants in the 2007 summit, categorized by topic. These obstacles subsequently serve as key points to guide participant recommendations.

Intelligence-led policing

Intelligence-led policing is at the core of the recommendations from the 2002 summit, yet the report from the 2002 summit does not attempt to define the term. Five years later, participants in the 2007 summit could not agree on a definition of intelligence-led policing. They made it clear that they believed that the nation's police departments as a group have not rushed to embrace intelligence-led policing, even as some progressive agencies have adopted it. The 2007 summit participants said the confusion about the nature of intelligence-led policing was just one of several reasons for the tepid response. They also cited a lack of awareness, indifference, and skepticism about another attempt to remake policing, and a concern that the name—intelligence-led policing—raises fears of government intrusions into the private lives of innocent persons and jeopardizes police relationships with constituents, especially members of minority groups.

Privacy, civil liberties, and civil rights

According to the 2007 summit participants, there is seldom a single set of privacy rules that control the way any given law enforcement agency can gather, store, and share information and intelligence. Instead, agencies must remain aware of sometimes overlapping privacy laws and regulations created by federal, state, and local authorities. As they negotiate these laws and regulations, law enforcement leaders are aware that they are part of a larger national debate about the gathering and use of information of all kinds. Nevertheless, they know that the complexity of today's threats to public safety and civil order demands new access to information.

Trust among police agencies

Participants in the 2002 summit expressed a concern that much criminal intelligence sharing is dependent on personal rather than institutional trust—that is, it occurs between agencies whose leaders have established collegial relationships but it seldom outlives the tenures of those leaders. Participants in the second summit in November 2007 said that has not changed much. Local, state, and tribal police leaders remain suspicious that federal agencies, in particular, withhold information and intelligence. Security classifications and clearances remain a point of contention among local, state, and tribal police leaders, some of whom complain that they cannot obtain clearances they should have and that too much information and intelligence is needlessly classified as Secret.

Law enforcement agencies remain somewhat reluctant to share information and intelligence with private sector security and other partners outside public law enforcement.

Information gathering and analysis

There persists among police leaders and their officers a lack of awareness of what information to gather and share, and among smaller agencies a sense that terrorism is a remote threat. Summit participants reported that analytical capacity has not expanded significantly across state, local, and tribal law enforcement agencies and that the need for analysis (as opposed to mere information retrieval and dissemination) is most acute in local and tribal police departments. Most U.S. police agencies are too small to employ any analysts and are unlikely to know where to find help with the analysis of information. Among larger agencies, few have a career path for the analysts they do hire, making it more difficult for them to recruit and retain analysts. Perhaps the most significant obstacle to improving analytical capacity is that many police managers do not have a consistent understanding of the role and value of analysts and their work.

Training

As evidenced by the work of Global, IALEIA, and their partners, training in criminal intelligence sharing exists for police employees at all levels—executives, managers, investigators, line officers, and analysts. Unfortunately, too few police officials know about it. Lack of awareness is just one barrier. Training, after all, takes time and money, two resources police departments have in short supply. Police executives at all levels acknowledge the difficulty of getting employees all the training they need and want, and criminal intelligence sharing is just one of many kinds of training police departments might desire but cannot always obtain.

Technology

Many agencies continue to rely on handwritten reports and paper-based records management systems, making information gathering, storage, retrieval, and sharing more difficult. Agencies might not be able to afford system upgrades that would allow participation in the NCISP and might not know how to go about it even if they could afford it. For other agencies, technology, such as computer database software, can sometimes seem to be an end in itself rather than the means, and agencies can sometimes mistake electronic information gathering and storage for analysis. Furthermore, some participants expressed continued frustration in accessing national level systems for intelligence sharing.

RECOMMENDATIONS

The participants in the 2007 Criminal Intelligence Sharing Summit developed the following recommendations to help U.S. law enforcement fully realize the NCISP and fulfill the promise of the 2002 summit recommendations. The 2007 recommendations include specific refinements of various elements of the plan, such as fusion centers, security clearances, and technology, but they emphasize the urgent need to engage every law enforcement agency, regardless of size and type, in criminal intelligence sharing. The two words spoken most frequently during the summit toward the engagement issue were marketing and training.

1.   Every state, local, and tribal law enforcement agency in the United States should strive to develop and maintain a criminal intelligence capability consisting of at least the following requirements: formal criminal intelligence awareness training for at least one sworn officer; training all levels of law enforcement personnel to recognize behavior indicative of criminal activity associated with terrorism; and defined procedures and mechanisms for communication with the nearest fusion center and/or a regional information sharing network.

No law enforcement agency is too small or too isolated to participate in criminal intelligence sharing. Experience has taught us that criminal and terrorist threats can develop in rural and suburban jurisdictions as readily as they can develop near urban targets. Indeed, terrorists have been known to live, work, and commit crimes in rural communities while they plan their attacks.

Participation is not costly and does not require a significant change in an agency's operations, nor does it require a law enforcement intelligence unit and a staff of analysts. Instead, participation for most of the nation's 18,000 law enforcement agencies concerns information, not intelligence, and requires the following elements:

- The chief executive's commitment to information sharing
- Basic criminal intelligence training for at least one sworn officer
- Training for all law enforcement personnel to recognize and report behavior and incidents indicative of criminal activity associated with international and domestic terrorism
- Participation in a regional information sharing network
- Periodic contact with the nearest fusion center to keep the lines of communication open
- Access to a legal advisor (such as corporate counsel) who can advise officers on the laws and regulations that restrict the gathering, use, and exchange of some kinds of information
- Engagement of community members with the agency in as many ways as possible (citizen advisory groups, citizen academies, emergency response teams, and so on)

Law enforcement officers in every agency are already trained to do the essential thing: spot suspicious activity. Participants suggested that officers need not become analysts of the information they gather about suspicious activity; they are busy enough with their primary responsibility of protecting public safety in their communities. But with the support of the chief executive and the guidance of an officer who understands the basics—what information to gather and how to gather it lawfully; what information to share and how to share it; and how to safeguard privacy and civil rights—every law enforcement officer can do his or her part to advance the cause of criminal intelligence sharing.

Fortunately, resources are available to help every agency participate in criminal intelligence sharing at a basic level, including training and support from law enforcement partners. The second recommendation of the 2007 summit participants is designed to help make every law enforcement agency aware of those resources.

2. A nationwide marketing and training initiative should be designed to convince every law enforcement agency to participate in criminal intelligence sharing, make every law enforcement agency aware of the criminal intelligence resources available to it, and give every law enforcement agency the know-how to participate in criminal intelligence sharing.

Participants in the 2007 summit agreed that many police executives, if not most, remain unaware of both their role in criminal intelligence sharing and the resources available to help them do their part. Much of what the nation's police agencies need—policy guidance, intelligence training, privacy and security standards, access to fusion centers, and so on—is already available or soon will be.

The IACP and other leadership organizations need to market criminal intelligence sharing to law enforcement executives and their officers, convince them of the need to participate in the process, and get the right resources into their hands. One outreach message could stress the need to attain at least a minimal criminal intelligence capability appropriate for a given agency's size and type. Most agencies, for instance, should strive to achieve at least a level 4 criminal intelligence capability—that is, assign criminal intelligence sharing responsibilities to at least one sworn officer and participate in a regional information sharing network.[15]

Summit participants were particularly focused on reaching the agencies that were likeliest to need the most support to participate in the plan: smaller police departments, tribal police departments, campus police departments, and other types of law enforcement agencies. The IACP and its partners, including Global, the COPS Office, PM-ISE, and IALEIA, are perhaps best situated to do that.

---

[15] U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Intelligence-Led Policing: A New Architecture,* in the series *New Realities: Law Enforcement in the Post–9/11 Era,* by IACP with the National Sheriffs Association, Major Cities Chiefs Association, Police Foundation, and NOBLE (Washington, D.C.: U.S. Government Printing Office, 2005), 13.

High-quality training on criminal intelligence sharing has been available from various sources for several years, but according to the participants in the 2007 summit, too few police executives know about the training and obtain it for their employees. The IACP, with unequaled access to the leaders of the nation's 18,000 law enforcement agencies, is in a position to change that. Together with its partners—the COPS Office, the DHS, Global, IALEIA, the International Association of Directors of Law Enforcement Standards and Training, and numerous others—the IACP could both promote participation in the criminal intelligence sharing plan and deliver training to law enforcement agencies everywhere.

Minimum training standards for criminal intelligence analysts, law enforcement executives, and other law enforcement officials involved in the intelligence process already exist. Global's *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States* recommends minimum standards for core competence for intelligence workers in each of six different classifications: intelligence analyst, intelligence manager, law enforcement executive, general law enforcement officer (basic and refresher training), criminal intelligence officer, and trainer.

As the authors of *Minimum Criminal Intelligence Training Standards* make clear, standards are not curricula. But they have helpfully included a suggested curriculum for each standard and refer the reader to additional sources of information. They also remind readers that the training content devised for each recipient should reflect both the latest national standards for criminal intelligence and the laws and regulations controlling criminal intelligence sharing in the jurisdiction in question.

Participants in the summit also recommend that some entity, such as the IACP and its partners, resolve the confusion surrounding the concept of intelligence-led policing. They were unable to agree on a definition of the term or settle on its core principles. As long as disagreement persists, it will be a distraction and an impediment to full participation in the NCISP.

3.   All law enforcement organizations and agencies should explore potential partnerships in order to enhance analytical capacity within their agencies.

Acknowledging that most of the nation's law enforcement agencies will focus on gathering and sharing information about suspicious criminal activity and will not be called on to produce finished criminal intelligence products, the 2007 summit participants also recognized that the growing number of agencies that do produce criminal intelligence for internal or external use need more analytical capacity. To achieve that, the summit participants recommended that the IACP and its partners take the specific steps listed below:

- Integrate the many analysis resources (including training) available from Global, IALEIA, the Federal Law Enforcement Training Center (FLETC), the Intelligence Training Master Calendar, and other sources.

- Promote the analytical standards established by Global, IALEIA, and others.

- Abide by minimum training standards for law enforcement criminal intelligence analysts and their clients in accordance with the *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*.

- Promote analyst professionalism through certification using the *Law Enforcement Analyst Certification Standards* developed by Global, such as the IALEIA Basic Analyst certification.

- Establish performance measures for qualitative and quantitative results.

4.   Chief executives of state, local, and tribal law enforcement agencies should encourage the directors of all criminal intelligence sharing initiatives and resources (such as fusion centers) to adopt and maintain an all-crimes approach.

Law enforcement agencies remain primarily concerned with preventing, detecting, and investigating crimes, enforcing traffic laws, promoting public safety, and working with community members to improve the quality of life in their jurisdictions. Terrorism is one of the many threats they deal with, and to some may seem like the most remote. These agencies are more likely to participate fully in criminal intelligence sharing, and therefore make fuller contributions to homeland security, if doing so helps them fulfill their primary mission. Some summit participants expressed concerns about fusion centers that restricted their work to terrorism exclusively. In their view, such a narrow focus is likely to discourage police participation. Fusion centers are run by state and local governments, and while the Federal Government is encouraging fusion centers to embrace an all-crimes and all-hazards approach, it does not have the authority to dictate a fusion center's mission or scope. Each fusion center sets its policies to best meet the needs of the agencies it supports. Fusion center directors and their law enforcement partners are responsible for determining what works best. The consensus among the summit participants was that an all-crimes approach works best, serving both local and national security interests.

5.   Fusion center directors and their law enforcement partners should take a series of steps to improve the effectiveness of the centers, including forming an association of fusion centers that might help promote the sharing of best practices among fusion centers and help promote the work of the centers to law enforcement agencies and policymakers at all levels.

Beyond adopting an all-crimes approach to information sharing, fusion center directors and law enforcement executives ought to reaffirm their commitment to working together to improve the utility of fusion centers. These steps reflect the belief that fusion centers must actively reach out to law enforcement agencies, some of whom may be unaware of their existence, do not know how to become involved, or may be operating under the misconception that they do not need to get involved with their local fusion center. Participants also called for law enforcement executives to not merely wait to hear from the nearest fusion center but to be proactive in their participation. To that end, the summit participants recommend the following action steps:

- Local, state, and tribal law enforcement leaders should define a process to ensure that suspicious activity reports (SARs) are made available to fusion centers in a timely manner.

- Fusion center directors should ensure that their centers are adhering to best practices for sustainability, privacy, performance measures, and analytic products.

- Fusion center directors should ensure that fusion centers adopt standards for records management.

- Fusion center directors should create advisory groups of practitioners to help guide the work of fusion centers in collaboration with the federal agencies that support the national network of fusion centers.

- Market fusion centers to local, state, and tribal police leaders, some of whom may be unaware of fusion centers and their roles and responsibilities.

- Equip fusion centers to receive and store classified information.

- Ensure that each fusion center creates a privacy officer position or assigns part-time privacy-officer responsibilities to a current staff member.

6.   The U.S. Department of Homeland Security, the Office of the Director of National Intelligence, the U.S. Department of Justice, and the National Guard should take steps to reduce barriers created by security classifications and clearances.

Participants in the 2007 summit noted that federal security clearances, security classifications, and secret/classified information networks posed barriers to non-federal agencies in criminal intelligence sharing and proposed the following action steps:

- Ensure the reciprocity of security clearances granted by DOJ, DHS, and the Department of Defense.

- Identify and create a ready reserve of state, local, and tribal investigators nationwide, give them appropriate clearances, and have local JTTFs brief the ready reserve on the status of ongoing investigations.

- Share unclassified versions of relevant classified products with local, state, and tribal police.

- Encourage all agencies to achieve at least a minimum level of computer technology and Internet access.

- Expedite the adoption of the federated ID and single sign-on.

Criminal intelligence officers and others rely on the availability of sensitive-but-unclassified (SBU) information stored in various networks, systems, and databases. Because most of these sources operate independently of the others, users typically must subscribe to each source separately and must therefore manage a different set of identification and sign-on credentials (such as usernames, passwords, and certificates) for each one. Separate credentialing is tedious for users and costly and inefficient for the operators of the SBU sources. A federated ID and single sign-on, such as the one developed and tested by the Global Federated Identity and Privilege Management (GFIPM) Security Interoperability Demonstration Project, could improve criminal intelligence sharing by allowing the user to enter just one set of credentials to gain access to all the participating SBU sources they wish to use. That simple step could make it easier for authorized users to obtain the information and intelligence they require[16] and make it more likely that they will leverage existing resources.

7.   Policy makers at the federal, state, local, and tribal levels should continue to take steps to enhance the protection of privacy, civil liberties, and civil rights and ensure that communities are aware of, and engaged in, the process.

Participants in the 2007 summit offered the following action steps with regard to protection of privacy, civil liberties, and civil rights:

- Engage community members in the work of each law enforcement agency in as many ways as possible (e.g., citizen advisory groups, citizen academies, emergency response teams).

- Ensure that every jurisdiction has a legal advisor (such as corporate counsel) who understands the laws and regulations controlling the gathering, use, and sharing of

---

[16] The Georgia Tech Research Institute (GTRI) Information Technology & Telecommunications Laboratory, *Project Report: Global Federation Identity and Privilege Management (GFIPM) Security Interoperability Demonstration,* submitted to the Global Justice Information Sharing Initiative, August 30, 2007, http://it.ojp.gov/documents/GFIPM_Security_Interoperability_Demonstration_Project_Report_2007-08-30.pdf.

information; the various safeguards in place to protect privacy and civil rights; and can advise law enforcement officers on these matters.

- Use the DHS/DOJ Fusion Process Technical Assistance Program's templates and checklists when developing privacy policies.[17]

- Ensure that every fusion center creates a privacy officer position or assigns part-time privacy officer responsibilities to a staff member.

8. Law enforcement executives should develop ways to measure the success of criminal intelligence sharing and recognize those individuals involved in that success.

If agencies reward officers primarily for arrests, duties like intelligence sharing that reduce officers' opportunities to make arrests also diminish their opportunities for recognition and advancement. Because each agency has its own way of recognizing achievement and its own intelligence capabilities and limitations, there can be no one-size-fits-all metric for criminal intelligence success. But there can nevertheless be an industry-wide commitment to measuring and recognizing the work of officers assigned to criminal intelligence capability.

---

[17] U.S. Department of Homeland Security and U.S. Department of Justice, Global Justice Information Sharing Initiative, *DHS/DOJ Fusion Process: Technical Assistance Program and Services* (October 2007), http://www.ise.gov/docs/misc/FusionProcessTechAssistance.pdf.

EPILOGUE

Since the November 2007 summit, a number of information sharing initiatives have emerged and expanded. We summarize some of these changes below:

Suspicious Activity Reporting (SARS)

To demonstrate how the concept of intelligence-led policing, as discussed in this report, can be deployed in an operational environment, DOJ, PM-ISE, and the FBI, in partnership with the Major Cities Chiefs Association (MCCA), IACP, and Global, embarked on an effort in the spring of 2008, to establish a national capacity for gathering, documenting, processing, analyzing, and sharing terrorism related suspicious activities reports—or Suspicious Activities Reports (SARs), as called for in the *National Strategy for Information Sharing*.

Supporting this effort is the Information Sharing Environment (ISE)-SAR Functional Standard, issued in January 2008, which defines both the data standards and business processes that will enable the sharing of terrorism-related SARs across the ISE— particularly between state and major urban area fusion centers and federal entities at the headquarters level.

In the spring of 2008, local best practices were identified regarding training front line personnel to recognize terrorism-related suspicious activities that may represent pre-incident indicators of a terrorism threat, and documenting those activities once observed. The results of this effort are documented in the draft June 2008 report, *Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project*.[18]

Building on the report's findings and recommendations, 12 state and local jurisdictions were selected to institute a standardized approach to gathering, documenting, processing, analyzing, and sharing terrorism related suspicious activities reports. Front line law enforcement personnel in these 12 locations will be trained to recognize behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Once reported or observed, behaviors and incidents indicative of criminal activity will be documented and evaluated by trained personnel to determine if they have a terrorism nexus. If a potential nexus with terrorism is established, the SAR will be made available to the local JTTF, regional and/or statewide fusion centers, and DHS.

Technical resources will be provided to enable the "posting" of terrorism-related SARs to a "shared space" in a manner consistent with technical standards contained within the ISE-SAR Functional Standard and its associated SAR Information Exchange Package Document. This will allow SARs to be accessed by other fusion centers,

---

[18] The report was approved by the Major Cities Chiefs Association on June 10, 2008, and is presented under review by the other partners involved in the project, to include the Criminal Intelligence Coordinating Council. Upon the partners' approval the report will be released publicly.

DHS Headquarters, other JTTFs to support regional and/or national analysis. Access to the "shared spaces" will be via LEO, RISSNET, and the Homeland Security Information Network (HSIN).

Protecting the information privacy and legal rights of Americans is a top priority. At the local level, SARs will be incorporated into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public. Additionally, SARs will receive multiple levels of review and vetting to ensure information is legally gathered and managed. Reports containing personally identifiable information that are determined to be unfounded, or that cannot be reasonably associated with criminal activity, will not be shared.

The PM-ISE and the ISE Privacy Guidelines Committee's (PGC) Legal Issues Working Group are in the process of completing an initial privacy and civil liberties review of the ISE-SAR Functional Standard and its implementation. The PGC will monitor this effort, provide advice and guidance to the project teams, and issue a final privacy and civil liberties analysis of the implementation of the ISE-SAR Functional Standard at the conclusion of the evaluation environment project.

The results of this initial phase will be documented to support the development and publication of an implementation guide and template for use by other state and local jurisdictions. Funding for this project is being provided by the PM-ISE and will be administered by BJA. The IACP, MCCA, Major County Sheriffs, and the CICC have been involved in planning and will be involved in implementation.

Baseline Capabilities for Fusion Centers

The *National Strategy for Information Sharing* identifies the development of baseline capabilities for fusion centers as a key step to reaching one of the Strategy's goals: "Establishing a National Integrated Network of State and Major Urban Area Fusion Centers." Over the past year, state and local fusion center personnel, with the support of their federal partners used the *Fusion Center Guidelines,* as well as identified best practices, to identify the capabilities and standards necessary for a fusion center to be considered capable of performing basic functions. The resulting document, *Baseline Capabilities for State and Major Urban Area Fusion Centers: An Addendum to the Fusion Center Guidelines,* is undergoing final review and is expected to be issued by Global this fall.

Defining these operational standards allows federal, state, and local officials to identify and plan for the resources needed - including financial and technical assistance, and human support - to achieve the Strategy's goal. By achieving this baseline level of capability, a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information. It will also support specific operational

capabilities, such as Suspicious Activity Reporting; Alert, Warning, and Notification; Risk Assessments; and Situational Awareness Reporting.

In support of the Strategy's goal, the Federal Government agreed that a "sustained federal partnership with state and major urban area fusion centers is critical to the safety of our nation, and therefore a national priority." While not all fusion centers receive federal grant funding, most fusion centers receive other types of support from the Federal Government including technical assistance, training, co-location of federal personnel, and access to federal information and networks. This document will help the Federal Government better identify how to support fusion centers and ensure they are providing the right types of resources in a consistent and appropriate manner. The capabilities also assist in ensuring that fusion centers have the basic foundational elements for integrating into the national ISE.

Law Enforcement Information Sharing Program (LEISP)

The Law Enforcement Information Sharing Program (LEISP) is DOJ's commitment to transform the way it shares law enforcement information with state, local, tribal and other federal law enforcement and homeland security partners. The Department's objective is to share information routinely across jurisdictional boundaries to prevent terrorism, and to systematically improve the investigation and prosecution of criminal activity. To achieve this objective, DOJ will put the right information into the hands of criminal investigators and analysts, whether they are on the street, in a command post, or working a task force. The following presents the status on key LEISP investments, as of June 2008.

National Data Exchange (N-DEx)

The FBI Criminal Justice Information Services Division has successfully launched the first increment of the National Data Exchange (N-DEx) in March 2008. Systems providing law enforcement data to N-DEx include but are not limited to the Delaware Criminal Justice Information System, the Automated Regional Justice Information System in Southern California, the Automated Regional Information Exchange System in Northern California, and the Oneida Nation. The N-DEx Program Management Office (PMO) continues to expand participation in N-DEx through outreach and training to federal, state, local, and tribal law enforcement organizations across the United States. Additionally, the N-DEx PMO continues to expand the capabilities and functions of the N-DEx system itself. The next major release of the system is scheduled for the middle of 2009.

OneDOJ (Formerly Regional Data Exchange or R-DEx)

OneDOJ is a DOJ repository for law enforcement information shared with other federal, state, local, and tribal law enforcement agencies through connections with regional

information sharing systems. OneDOJ serves as DOJ's system to share criminal law enforcement information internally across investigative components and provide regional criminal law enforcement connectivity for authorized users to conduct federated searches of OneDOJ information.

All DOJ law enforcement components – ATF, BOP, DEA, FBI, and USMS - are sharing information under consistent policy and technical standards. Information shared includes open and closed case documents, investigative reports, witness interviews, criminal event data, criminal history and incarceration information, and identifying information about individual offenders. Recently, the OneDOJ system has expanded the quantity and quality of DOJ law enforcement data and expanded regional law enforcement information sharing partnerships around the country. The Department through the OneDOJ system is sharing information with the following organizations.

OneDOJ Partners

Naval Criminal Investigative Service

The Naval Criminal Investigative Service (NCIS) is the investigative arm of the Department of Navy. As part of the Law Enforcement Information Exchange (LInX) initiative, NCIS has created strategically placed information hubs that provide participating agencies with secure access to regional crime and incident data. Connectivity between LInX locations and OneDOJ are in place for the following six regional locations: Northwest, Gulf Coast, National Capitol Region, Southeast, Hampton Roads, and Hawaii.

Department of Homeland Security

The Immigration and Customs Enforcement (ICE) is the largest investigative arm of DHS. ICE is responsible for eliminating vulnerabilities in the nation's border, and with economic, transportation and infrastructure security. As part of the DHS Law Enforcement Information Sharing Strategy, ICE created the Immigration and Customs Enforcement Pattern Analysis and Information Collection System (ICEPIC). ICEPIC is used to identify relationship patterns that are indicative of violations of U.S. customs and immigration laws and possible terrorist activities, potentially resulting in the opening of new investigative cases. DHS and DOJ fostered a partnership to share law enforcement information and where practical to share connectivity resources to various state, local, and tribal regional information sharing consortia.

State, Local, and Tribal Partners

OneDOJ has established formal partnerships with regional law enforcement information sharing consortia around the country. The aforementioned locations initiated by NCIS lists several where OneDOJ has created formal partnership through

a Memorandum of Understanding. The following are other regional law enforcement information sharing partnerships.

- Los Angeles Sheriff's Department
- St. Louis, MO (Crime Matrix)
- San Diego Regional Law Enforcement Consortium (Automated Regional Justice Information System)

National Information Exchange Model (NIEM)

The National Information Exchange Model (NIEM) is a national model that eases cross-domain exchanges. It is a standard vocabulary that is used to define Information Exchange Package Documentation (IEPD). As such, one IEPD that is based on NIEM is the Law Enforcement Exchange Specification (LEXS). LEXS (pronounced "lex") codifies the objectives of LEISP and enables DOJ and other federal, state, local, and tribal law enforcement organizations to utilize the specification to establish law enforcement information exchanges. LEXS is the basis for the aforementioned OneDOJ regional law enforcement information sharing partnerships. Other results from NIEM and LEXS include the following:

- A specification was developed based on LEXS for suspicious activity reports. This will allow federal, state, local, and tribal officials to share information on suspicious activities in a consistent and repeatable manner.

- The LEISP Program Management Office continues to collaborate with industry, federal, state, local, and tribal partners on the LEXS implementations.

IACP Summit Staff and Consultants

<u>Executive Staff</u>

Daniel N. Rosenblatt   Executive Director
James M. McMahon   Deputy Executive Director
John Firman   Director of Research

<u>Breakout Session Facilitators</u>

Bart Johnson, Office of the Director of National Intelligence (formerly with, New York State Police)
Deputy Chief Mike Downing, Los Angeles Police Department, California
Chief of Detectives Peter Modafferi, Rockland County District Attorney's Office, New York
Assistant Director Russell Porter, Intelligence Bureau Chief, Iowa Department of Public Safety
Alexander Joel, Esquire, Civil Liberties Protection Officer, Office of the Director of National Intelligence
Kenneth Mortensen, Acting Chief Privacy and Civil Liberties Officer, U.S. Department of Justice
 J. Patrick McCreary, Associate Deputy Director, Policy Office, Bureau of Justice Assistance, U.S. Department of Justice
Chief Yousry Zakhary, Woodway Department of Public Safety, Texas
Lisa Palmieri, President, International Association of Law Enforcement Intelligence Analysts (IALEIA)
Colonel Joseph Fuentes, Superintendent, New Jersey State Police
Commissioner Kerry Sleeper, Homeland Security Advisor, Vermont Department of Public Safety
Chief Joseph Polisar, Garden Grove Police Department, California

<u>Breakout Session Support Staff</u>

Heather Ruzbasan Cotter, Coordinator
Chuck Everhart, System Software Manager
Suzy Jordan, Project Manager
Clarence Bell, Manager
Laura Bell, Training Coordinator
Phil Lynn, Manager
Tamika Scott, Technical Assistance Coordinator
Elaine Deck, Sr. Program Manager
Kristen Beam, Project Manager
Aviva Kurash, Project manager
Vince Talucci, Director State and Provincial Police
Cynthia Schauman, Project Assistant
John Markovic, Program Manager

Mike Fergus, Project Manager
Jack Grant, Sr. Program Manager
Suzy Jordan, Project Manager
Dianne Beer-Maxwell, Project Manager
Amanda L. Cardone, Training Coordinator
Ian Hamilton, Project Coordinator

Summit Coordination

Katerina Karakehagia, Research Center Coordinator

Logistical Support

Eleni Trahilis, Research Intern
Dorothy Yeung, Research Intern

Report Writer

Gregg Walker

Editorial Staff

Gene Voegtlin
Wendy Balazik
Tracy Phillips

SUMMIT PARTICIPANTS

Ms. Judy Abney
Policy and Planning Division
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Chief Richard T. Ahlstrom
Administration
Cedar Falls Police Department

Mr. Charles Allen
Chief Intelligence Officer
Office of Intelligence and Analysis
U.S. Department of Homeland Security

Deputy Chief Robert Allen
Patrol Bureau
Minneapolis Police Department

Mr. John Awtrey
Director
Law Enforcement Policy and Support
U.S. Department of Defense

Sheriff Leroy D. Baca
Los Angeles County Sheriff's
Department

Ms. Kristen Beam
Former Project Manager
Gun Violence Reduction Initiative
International Association of Chiefs of
Police

Mr. Christian Beckner
Democratic Professional Staff Member
Senate Homeland Security and
Governmental Affairs Committee

Ms. Dianne Beer-Maxwell
Project Manager
New Police Chief Mentoring Project
Research Center Directorate
International Association of Chiefs of
Police

Mr. Clarence W. Bell
Grant Technical/Management S&P
Manager
State and Provincial Police Division
International Association of Chiefs of
Police

Ms. Laura P. Bell
Training Coordinator
Technology Technical Assistance
Program
International Association of Chiefs of
Police

Chief William B. Berger
Executive Division
Palm Bay Police Department

Major George L. Bivens
Director, Intelligence Division
Bureau of Criminal Investigation
Pennsylvania State Police

Mr. Doug Bodrero
Institute for Intergovernmental Research

Mr. Robert P. Boehmer
Chair, Global Advisory Committee
Institute for Public Safety Partnerships
University of Illinois at Chicago

Major Robert W. Booker
Commander
Office of Investigative Services
Ohio State Highway Patrol

Mr. Leonard C. Boyle
Director
Terrorist Screening Center

Ms. Kelly Brickley
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Ronald E. Brooks
Director
Office of National Drug Control Policy
Northern California High Intensity Drug
Trafficking Area

Mr. James H. Burch
Deputy Director
Bureau of Justice Assistance
U.S. Department of Justice

Ms. Valerie Calogero
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Ms. Pamela Cammarata
Associate Deputy Director
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Captain Leslie M. Campbell
Mass Transportation Liaison
Support Services Bureau
Metro Transit Police Department

Mr. Glenn M. Cannon
Assistant Administrator
Disaster Operations Directorate
Federal Emergency Management
Agency

Ms. Amanda L. Cardone
Training Coordinator
Research Center Directorate
International Association of Chiefs of
Police

David L. Carter, Ph.D.
Director/Professor
Intelligence Program
School of Criminal Justice
Michigan State University

Chief Salvatore Cassano
New York City Fire Department

Mr. Frank Cilluffo
Associate Vice President and Director
Homeland Security Policy Institute
The George Washington University

Mr. Ken Clark
Technology Division
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. John Cohen
Senior Advisor
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. R. Scott Crabtree
Director
Business Processes Division
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Bob Cummings
Institute for Intergovernmental Research

Ms. Heather J. Davies, Ph.D.
Policy and Planning Division
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Ms. Elaine F. Deck
Senior Program Manager
Research Center Directorate
International Association of Chiefs of
Police
515 North Washington Street

Commander David Denlinger
Intelligence Bureau
Arizona Department of Public Safety

Mr. Charles Dinse
Law Enforcement Advisor to the
Administrator
Office of the Administrator
Federal Emergency Management
Agency

Mr. Dave Divalerio
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Brian Dodwell
Terrorism Prevention Exercise Program
Manager
National Preparedness Directorate
Federal Emergency Management
Agency

Chief Harry P. Dolan
Raleigh Police Department

Mr. Joseph E. Donovan
Acting Assistant Director
Intelligence Division
National Drug Intelligence Center

Deputy Chief Michael Downing
Counter-Terrorism and Criminal
Intelligence Bureau
Los Angeles Police Department

Mr. Theodore Duncan
Deputy Assistant Director
Intelligence Programs Division
Immigration and Customs Enforcement
U.S. Department of Homeland Security

Mr. Charles S. Eaneff
Distinguished Fellow
Office of the Administrator
Federal Emergency Management
Agency

Mr. Chuck Everhart
System Software Manager
International Association of Chiefs of
Police

Commissioner Julian Fantino
Ontario Provincial Police

Ms. Elizabeth Farrell
Communications and Outreach
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Michael Fergus
Project Manager
Video Evidence Projects
International Association of Chiefs of
Police

Director Tom Finan
Subcommittee on Intelligence,
Information Sharing, and Terrorism
Risk Assessment
Committee on Homeland Security

Mr. John Firman
Director of Research
Research Center
International Association of Chiefs of
Police

Captain Kenneth D. Fitzgerald
Investigations Division
Danville Police Department

Ms. Christine Fletcher
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Police Commissioner Edward A. Flynn
Springfield Police Department

Colonel Joseph R. Fuentes
Superintendent
New Jersey State Police

Mr. Chuck Gardner
Business Process
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Ms. Kimberly Geer
Institute for Intergovernmental Research

Assistant Chief Ralph L. Godbee, Jr.
Administrative Portfolio
Detroit Police Department

Deputy Chief David Lacy Graham
Investigations Service Group
Charlotte-Mecklenburg Police
Department

Mr. Jack C. Grant
Senior Program Manager
Research Center Directorate
International Association of Chiefs of
Police

Commander Michael Grossman
Office of Homeland Security
Los Angeles County Sheriff's
Department

Mr. Raymond Guidetti
Detective Sergeant First Class
New Jersey Regional Operations
Intelligence Center
New Jersey State Police

Director David Hagy
National Institute of Justice
Office of Justice Programs
U.S. Department of Justice

Mr. Ian Todd Hamilton
Project Coordinator
Research Center Directorate
International Association of Chiefs of
Police

Mr. Stephen Henderson
Office of Intelligence
Immigration and Customs Enforcement
U.S. Department of Homeland Security

Captain W. Todd Henry
Specialized Investigations Division
Metro Nashville Police Department

Captain Richard W. Holland
Criminal Intelligence
Houston Police Department

Mr. Dave Hong
Technology Division
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Kevin Jackson
Deputy Assistant Director
Business Management and Budget
Division
Immigration and Customs Enforcement
U.S. Department of Homeland Security

Chief Kenneth B. James
Flandreau Police Department

Chief Wayne M. Jerman
Assistant Chief of Police
Investigative Services Bureau
Montgomery County Department of
Police

Alexander Joel, Esquire
Civil Liberties and Privacy Office
Office of the Director of National
Intelligence

Mr. Bart R. Johnson
Director of Homeland Security and Law
Enforcement
Office of the Director of National
Intelligence

Mr. Nate Jones
Counsel to Senator Kohl
Committee on the Judiciary
United States Senate

Ms. Suzanne E. Jordan
Project Manager
Research Center Directorate
International Association of Chiefs of
Police

Ms. Katerina Karakehagia
Research Center Coordinator
Research Center Directorate
International Association of Chiefs of
Police

Assistant Chief Dave J. Karnitz
Investigative Services Bureau
Washington State Patrol

Mr. David Kaufman
Director
Preparedness Policy, Planning, and
Analysis
National Preparedness Directorate
Federal Emergency Management
Agency

Commander Jon Kehrberg
Investigations Division
Chaska Police Department

Mr. Phil Keith
Project Director
Intelligence-Led Policing
Major Cities Chiefs Association

Mr. Scott H. Kelberg
Grants Development and Administration
Federal Emergency Management
Agency

Mr. Aaron D. Kennard
Executive Director
National Sheriffs' Association

Mr. Donald F. Kennedy
Executive Director
New England State Police Information
Network
Regional Information Sharing Systems

Chief Gil Kerlikowske
Seattle Police Department

Sheriff James F. Kralik
Sheriff Administration
Rockland County Sheriff's Department

Ms. Aviva Kurash
Project Manager
Research Center Division
International Association of Chiefs of
Police

Chief Russell B. Laine
Algonquin Police Department

Mr. Andrew L. Lluberes
Director
Communications for Intelligence and
Analysis
Office of Public Affairs
U.S. Department of Homeland Security

Mr. Chester F. Lunner
Deputy Assistant Secretary
Office of Intelligence and Analysis
U.S. Department of Homeland Security

Mr. Philip L. Lynn
Manager
National Law Enforcement Policy
Center
International Association of Chiefs of
Police

Colonel Thomas F. MacLeish
Superintendent
Department of Safety and Homeland
Security
Delaware State Police

Acting Chief Paul S. MacMillan
Massachusetts Bay Transportation
Authority
Transit Police Department

Chief David L. Maggard, Jr.
Administration
Irvine Police Department

Mr. Tom Malarkey
Business Process
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. John D. Markovic
Program Manager
Programs and Research
International Association of Chiefs of
Police

Mr. Richard H. L. Marshall
Senior Information Assurance
Representative
Office of Legislative Affairs
National Security Agency

Captain J. Thomas Martin
Commander
Criminal Intelligence Division
Bureau of Criminal Investigation
Virginia State Police

Ms. Tarrazzia Martin
Director, Policy and Programming
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Commander Jefferson L. Massie
Intelligence Division
Orange County Sheriff's Office

Chief Kent W. Mawyer
Criminal Law Enforcement Division
Texas Department of Public Safety

Mr. Edward P. McCarroll
Supervisory Intelligence Operations
Specialist
Office of Intelligence and Analysis
U.S. Department of Homeland Security

Mr. J. Patrick McCreary
Associate Deputy Director
Bureau of Justice Assistance
Office of Justice Programs
U.S. Department of Justice

Assistant Commissioner Mike
McDonell
National Security Criminal
Investigations
Royal Canadian Mounted Police

Mr. James McMahon
Deputy Executive Director
International Association of Chiefs of
Police

Ambassador Ted E. McNamara
Program Manager, Information Sharing
Environment
Office of the Director of National
Intelligence

Ms. Katherine McQuay
Supervisory Special Analyst
Office of Community Oriented Policing
Services
U.S. Department of Justice

Mr. Chuck Miller
Office of Policy and Interagency Affairs
National Drug Intelligence Center
U.S. Department of Justice

Ms. Michelle Miller
Institute for Intergovernmental Research

Mr. Sid Mitchell
First Vice President
Executive Board
Federal Bureau of Investigation
National Academy Associates

Chief of Detectives Peter A. Modafferi
Investigations Bureau
District Attorney's Office
County Courthouse

Mr. William A. Morange
Director of Security
Security Department
Metropolitan Transportation Authority

Mr. Barry Morgan
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Kenneth Mortensen
Acting Chief Privacy and Civil Liberties
Officer
Office of the Deputy Attorney General
U.S. Department of Justice

Mr. Vic Mukai
Information Sharing Environment,
Program Management Office
Scitor Corporation

Mr. Wayne Murphy
Assistant Director
Directorate of Intelligence
Federal Bureau of Investigation

Mr. Michael Muth
Assistant Director
State and Local Liaison Division
INTERPOL-Washington
U.S. Department of Justice

Mr. Jerry Needle
International Association of Chiefs of
Police

Chief Daniel Oates
Police Administration
Aurora Police Department

Chief Thomas P. O'Connor
Maryland Heights Police Department

Mr. Thomas O'Reilly
Senior Policy Advisor
Bureau of Justice Assistance
U.S Department of Justice

Director Dwayne Orrick
Public Safety Director
Administration
Cordele Police Department

Chief Neil Ouellette
Administration
Danvers Police Department

Ms. Lisa M. Palmieri
President,
International Association of Law
Enforcement Intelligence Analysts
(IALEIA)

Director Carl Peed
Office of Community Oriented Policing
Services
U.S. Department of Justice

Mr. Earl O. Perkins
Deputy Superintendent
Boston Regional Intelligence Center
Boston Police Department

Chief Doug H. Pettit
Oregon Police Department

Sergeant Julio R. Pinera
Supervisor
Special Investigations Section
City of Miami Police Department

Mr. John Pistole
Deputy Director
Federal Bureau of Investigation

Chief Joseph Polisar
Garden Grove Police Department

Mr. Russell M. Porter
Director
Iowa Fusion Center
Iowa Department of Public Safety

Chief Joseph R. Price
Leesburg Police Department

Mr. David J. Pyle
Senior Intelligence Advisor
Policy, Plans, and Requirements
Directorate
Office of the Director of National
Intelligence

Mr. Tim Quinn
Office of Community Oriented Policing
Services
U.S. Department of Justice

Ms. Diane Ragans
Institute for Intergovernmental Research

Dr. Jerry Ratcliffe
Professor
Department of Criminal Justice
Temple University

Director Edward Reina
Department of Public Safety
Tohono O'odham Nation

Ms. Sue Reingold
Deputy Program Manager
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Mr. Robert C. Riegle
Director
State and Local Program
Office of Intelligence and Analysis
U.S. Department of Homeland Security

Mr. Warren J. Riley
Superintendent of Police
New Orleans Police Department

Chief Susan Riseling
Vice President at Large, International
Association of Chiefs of Police
University of Wisconsin-Madison Police
Department

Chief Raymond J. Rose
Mundelein Police Department
Village of Mundelein

Mr. Dan Rosenblatt
Executive Director
International Association of Chiefs of
Police

Director Ronald C. Ruecker
President, International Association of
Chiefs of Police
Public Safety Division
City of Sherwood

Ms. Heather Ruzbasan Cotter
State and Provincial Police Division
International Association of Chiefs of
Police

Mr. Kevin M. Saupp
Section Chief, Prevention and Protection
National Preparedness Directorate
U.S. Department of Homeland Security

Ms. Amy Schapiro
Senior Social Science Analyst
Office of Community Oriented Policing
Services
U.S. Department of Justice

Ms. Cynthia Schauman
Research Division
International Association of Chiefs of
Police

Dr. Matthew C. Scheider
Assistant Director
Office of Community Oriented Policing
Services
U.S. Department of Justice

Mr. Kurt F. Schmid
Senior Law Enforcement Advisor
Counterdrug Technology Assessment
Center
White House Office of National Drug
Control Policy

Chief Paul D. Schultz
Police Administration
Lafayette Police Department

Chief James Schwartz
Arlington County Fire Department

The Honorable Marie O'Neill Sciarrone
Special Assistant to the President and
Senior Director for Cybersecurity and
Information Sharing Policy
Homeland Security Council
The White House

Ms. Tamika Scott
Technical Assistance Coordinator
Research Division
International Association of Chiefs of
Police

Colonel Terrence B. Sheridan
Superintendent
Maryland State Police

Commissioner Kerry L. Sleeper
Department of Public Safety
Vermont State Police

Dr. Clark Smith
Director, Technology Division
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Sheriff Richard W. Stanek
Administration
Hennepin County Sheriff's Office

Mr. Dana V. Starks
Interim Superintendent
Chicago Police Department

Mr. Chips Stewart
The CNA Corporation

Commissioner Frank G. Straub
Department of Public Safety
City of White Plains

Mr. Vincent Talucci
Director
State and Provincial Police Division
International Association of Chiefs of
Police

The Honorable Frances Fragos
Townsend
Assistant to the President
Homeland Security and
Counterterrorism
The White House

Ms. Eleni Trahilis
Research Center
International Association of Chiefs of
Police

Director Larry G. Trent
Illinois State Police

Assistant Commissioner Ken S. Tucker
Office of Executive Director
Florida Department of Law
Enforcement

Chief Gary L. Vest
Administration
Powell Police Department

Mr. Gene Voegtlin
International Association of Chiefs of
Police

Mr. Gregg A. Walker
G. W. & Associates, LLC

Chairman Robert Wasserman
Strategic Policy Partnership

Commander David A. Webb
Criminal Investigation Division
Metro Transit Police Department

Ms. Sandra Webb
Deputy Director
Office of Community Oriented Policing
Services
U.S. Department of Justice

Sheriff Craig Webre
President, National Sheriffs' Association
Lafourche Parish Sheriff's Office

Dr. Josh Weerasinghe
Senior Advisor
Office of the Program Manager,
Information Sharing Environment
Office of the Director of National
Intelligence

Chief John Welter
Anaheim Police Department

Chief Wesley Wilson
Information Sharing Program Office
National Counterterrorism Center

Mr. Jim Woosley
Acting Assistant Director of Operations
Office of Intelligence
Immigration and Customs Enforcement
U.S. Department of Homeland Security

Ms. Dorothy Yeung
Research Center Directorate
International Association of Chiefs of
Police

Chief Yousry A. Zakhary
State Associations of Chiefs of Police
Woodway Department of Public Safety