LEISP:

United States Department of Justice Law Enforcement Information Sharing Program

October 2005

Foreword

The Department of Justice (referred to herein as "DOJ" or "Department") is transforming the way it shares law enforcement information with its federal, state, local, and tribal law enforcement partners. The vision is to create relationships and methods that allow information to be shared routinely across jurisdictional boundaries to prevent terrorism and to systematically improve the investigation and prosecution of criminal activity.

The Department will achieve its vision by formulating information sharing policies and standard business practices and by creating a unified, Department-wide technology architecture that will position DOJ as a committed partner in an information sharing environment of federal, state, local, and tribal law enforcement agencies.

The strategy for DOJ's transformation is expressed through the Law Enforcement Information Sharing Program (LEISP). This strategy is the result of a collaborative process involving senior leadership from DOJ component agencies and representatives from across the national law enforcement community. LEISP is also the Department's strategy for sharing DOJ data – from all its components – with the Information Sharing Environment (ISE) mandated by the Intelligence Reform and Terrorism Prevention Act of 2004.

LEISP is a program, not an information "system." It addresses barriers to information sharing and creates a forum for collaboration on how existing and planned systems will be coordinated and unified for information sharing purposes. LEISP delineates guiding principles, a policy framework and functional requirements that are necessary to facilitate multi-jurisdictional law enforcement information sharing. LEISP establishes DOJ's commitment to move from a culture of "need to know" toward a culture of "need to share" in which information is shared as a matter of standard operating procedure. Through the strategy, DOJ also commits to participate as a partner to help bring together the law enforcement community in the common cause of achieving multi-jurisdictional information sharing.

LEISP sets in motion three implementation tracks: Track I is the Department's internal reform initiative, OneDOJ, which will closely coordinate information sharing efforts within the Department, facilitate sharing of DOJ-held information with law enforcement agencies outside the Department, provide connectivity for sharing of information with the Department of Homeland Security (DHS) and allow DOJ to present a single face to its information sharing partners. Track II will first incorporate "quick hits" to leverage existing sharing-technology capabilities and then center on building out the services and technology platforms that will enable the Department to seamlessly share its information. In Track III, the Department will work cooperatively with its federal, state, local, and tribal law enforcement partners to enhance interconnectivity that allows standard, routine information sharing across all jurisdictions on a national basis.

DOJ has circulated this LEISP strategy to representatives of law enforcement across the United States. The Department appreciates the assistance of the Global Advisory Committee and the Criminal Justice Information Services Advisory Policy Board (CJIS APB) in facilitating the collaboration process.

Table of Contents

1. Strategy Context

The goal of the Law Enforcement Information Sharing Program (LEISP) strategy is to enable DOJ to share law enforcement information with its federal, state, local, and tribal law enforcement partners and to facilitate multi-jurisdictional information sharing across the law enforcement and homeland security communities. The strategy formulates new DOJ law enforcement information sharing policies and business processes as well as a Department-wide technology architecture aimed at confronting identified barriers to routine information exchange. When executed, the strategy will establish the Department as a committed partner in an information sharing environment of federal, state, local, and tribal law enforcement agencies, where the power of information is marshaled to support the shared mission of preventing and prosecuting terrorism and all criminal activity.

1.1 Building on Information Sharing Strengths

Law enforcement agencies have been collecting and sharing information for decades. To support law enforcement needs, DOJ and other law enforcement agencies have been providing actionable information that supports the mission and objectives of law enforcement agencies at all levels, by providing a variety of information sharing programs. For example, the FBI's Criminal Justice Information System (CJIS)[1] provides law enforcement information relating to criminal histories, uniform crime reporting and fingerprint identification to meet the needs of federal, state, local, and tribal law enforcement agencies. State, local, and tribal law enforcement partners adhere to the CJIS programs, systems, and requirements for information sharing and summary data reporting. The state and local data providers and systems users share responsibility for the operation and management of CJIS with the FBI through the CJIS Advisory Policy Board (CJIS APB). This shared management approach has provided the blueprint for the beginning of one of the most important prerequisites of successful information sharing: a federation of trust among all parties in the CJIS information sharing community.

Another example of successful information sharing among law enforcement is the National Law Enforcement Telecommunications System (NLETS). This system is the electronic backbone for connecting state and local agencies and services for a majority of interstate and national law enforcement information sharing. NLETS is wholly owned and operated by the states and works cooperatively with the FBI and the CJIS APB in setting evolving and shared standards for connectivity and communication.

Notwithstanding these and other successes, however, highly sophisticated and rapidly evolving terrorist and criminal activities now present threats to our nation’s internal peace and security that make dramatic and far-reaching improvements to information sharing a national imperative. To be successful, government must build on the current successful business processes while effectively addressing new and longstanding challenges.

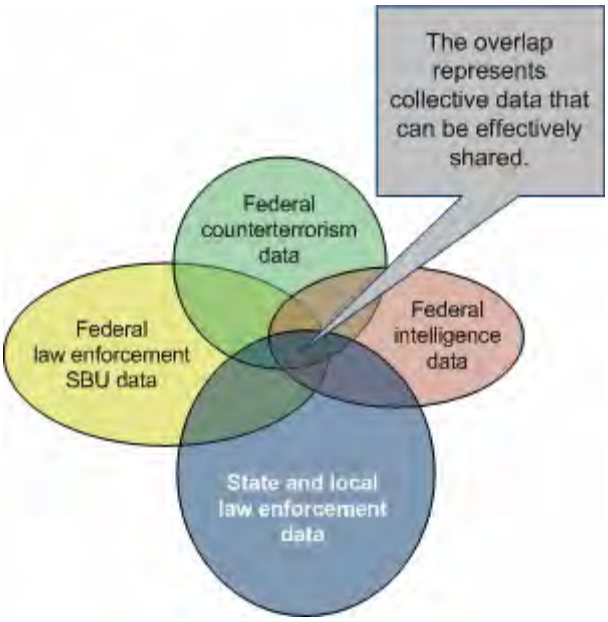
[1] CJIS serves as the focal point and central repository for criminal information services, and oversees the National Crime Information Center (NCIC), Uniform Crime Reporting (UCR), and Fingerprint Identification. In addition, CJIS is responsible for several ongoing technological initiatives, including the Integrated Automated Fingerprint Identification System (IAFIS), NCIC 2000, and the National Incident-Based Reporting System (NIBRS).

1.2 Challenges

Notwithstanding examples of successful information sharing, the current environment requires the adoption of an entirely new paradigm for information sharing. Current information collection and dissemination practices have not been planned as part of a unified national strategy but rather have evolved incrementally over time to meet certain needs or address specific challenges as they have surfaced. While sharing does occur through these stovepiped efforts, it is commensurately limited in degree and effectiveness. A tremendous quantity of information that *could* be shared is still not *effectively* shared and utilized among the various law enforcement communities.

Previous efforts to improve this situation have been beset by a multitude of challenges. The LEISP strategy addresses both the new and longstanding challenges to information sharing. These challenges include: increasing sophistication and complexity of terrorist and criminal organizations; the highly fragmented and autonomous nature of law enforcement; inadequacy of existing information systems; lack of consistent policies and practices; interagency mistrust; categorization of otherwise shareable information into non-shareable categories; and the need to coordinate information sharing efforts.

Figure 1-1: Current State of Law Enforcement Information Sharing



1.2.1 Increasing Sophistication and Complexity of Terrorist and Criminal Organizations

Criminal and terrorist organizations have become increasingly complex. They are more sophisticated, mobile and networked, while law enforcement has remained stovepiped and relatively disconnected. This evolving complexity obscures relationships and activities,

inhibiting the ability of law enforcement to obtain the information needed to link facts and discover patterns to more effectively combat criminal activity and terrorism.[2]

1.2.2 Highly Fragmented and Autonomous Nature of Law Enforcement

The United States is premised on a system of federal governance where power is divided between the national and regional governments. The checks and balances this federal structure provides have served the nation well and are an essential component of America's culture, fundamental to the protection of basic rights and the foundation of much of the strength, resiliency, and success of our system of government. However, it also means that law enforcement is organized into over 18,000 separate state, local, and tribal jurisdictions, with independent governance, information systems, and activities, and subject to their own set of circumstances, concerns, and limitations. The multiplicity of jurisdictions and their autonomous nature engender inconsistent policies, practices, and systems, and make coordination among agencies difficult. It also means that no one entity can mandate coordination across all agencies.

This situation has created many longstanding challenges to information exchange and presents additional challenges when attempting to mitigate such barriers. This challenge has existed for some time, but with the advent of increased sophistication of criminals, it becomes a serious vulnerability that terrorist and criminal agents can exploit to shield their activities from detection and prosecution. The jurisdictional boundaries can themselves become walled-off enclaves that present significant barriers to information sharing. As a result, it becomes difficult for law enforcement to "connect the dots" across jurisdictions or activities, increasing the ability of terrorists and criminals to plan and perpetrate malevolence.

1.2.3 Lack of Consistent Policies and Practices

Due to a lack of consistent policy framework across law enforcement, information sharing practices and policies vary from agency to agency in regard to such issues as privacy protection, security, data quality control, and access. These inconsistent approaches make it difficult – and sometimes illegal – to share information with other agencies. For example, one jurisdiction may be unable to share information because the receiving jurisdiction does not meet required conditions for privacy, security or access protection. Conflicts between freedom of information, privacy policies, and security policies could mean that sensitive law enforcement information cannot be shared with another jurisdiction.

1.2.4 Inadequate Information Systems

Another result of the multiplicity of independent agencies is a lack of common standards and policies for information exchange. Inconsistent practices continue to hinder information sharing today. Despite efforts to coordinate and integrate, law enforcement information systems have been developed without the benefit of an overarching national information sharing strategy. Existing information technology systems were designed to address needs and exigencies of the time for specific agencies or jurisdictions. Most systems were not built to exchange information across agencies. As a result, law enforcement information systems remain stovepiped, with

[2] Accordingly, addressing law enforcement information sharing is now more important than ever, constituting a critical and national imperative. Moreover, new tools for "connecting the dots" are needed so that law enforcement can more effectively deal with the sophisticated threats that exist.

limited interoperability and connectivity, inadequate for effective information sharing of the kind and magnitude needed today.

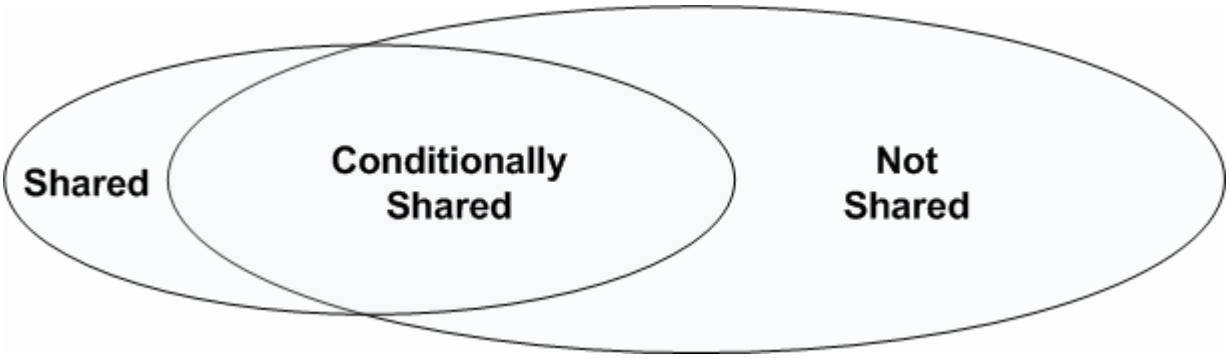
1.2.5 Interagency Mistrust

As a result of inconsistent policies and practices, those who do share sensitive information cannot always be sure how it will be used, that it will be protected, or who will ultimately have access to it. The ensuing uncertainty creates a climate of wariness and mistrust among agencies. These legitimate concerns can make agencies reluctant to share their information and unwilling to participate fully in information sharing initiatives.[3] This legacy of institutional mistrust has undermined previous information sharing efforts and now constitutes one of the most intractable barriers to improving information sharing.

1.2.6 Categorization of Otherwise Shareable Information into Non-shareable Categories

Another barrier to information sharing is created when information that should be categorized as shareable is categorized in a way that precludes it from being shared. For example, otherwise unclassified information uncovered in the course of a classified investigation may become classified because the entire case is classified. While procedures are in place to address this, such as issuing redacted versions of classified information (so-called tearline[4] versions), these efforts take time and require significant resources. In addition, legitimate concerns over the use of information in operations can also contribute to over-classification. Consequently, not withstanding those procedures, much shareable information is not currently shared due to the application of restrictive categorizations. This situation is depicted in Figure 1-2 below:

Figure 1-2: Current Information Sharing Paradigm



1.2.7 Need to Coordinate Information Sharing Efforts

In the past, many studies, strategies, and initiatives have been developed to address these issues, but they too have been beset by the vagaries of the very fragmentation they are designed to

[3] Where information sharing is working well, it is sometimes because individual trusted relationships have been leveraged to transcend institutional uncertainty and mistrust.

[4] Creating a "tearline" is the process of reviewing classified information and presenting information that is suitable for dissemination in a redacted format. The term derives from the practice of placing this redacted information physically below the classified information on a document with a tearline so information that was suitable for dissemination can be easily identified.

address. These initiatives have focused on either a single region of the country or limited types of information. In many cases, regional initiatives have not been coordinated with one another.

Since the terrorist attacks of September 11, 2001, the President and Congress have sought to address these challenges by mandating information sharing and directing cooperation among agencies. The law enforcement community has responded in turn with a new wave of regional and national information sharing initiatives. Numerous groups have put forth these initiatives and plans. A non-comprehensive sample includes:

- Global Justice Information Sharing Initiative
- National Criminal Intelligence Sharing Plan
- Markle Foundation Task Force: Creating A Trusted Network For Homeland Security
- 9/11 Commission Report and Recommendations
- Law Enforcement Regional Data Exchange
- Intelligence Community Information Sharing Working Group
- Community Interoperability and Information Sharing Office Policy Board
- DOJ-DHS Ad Hoc Working Group on SBU-level Information Sharing Systems
- National Virtual Pointer System Coordinating Committee
- Justice Intelligence Coordinating Council
- Homeland Security Advisory Council Working Group
- National Association of State Chief Information Officers

The sheer number of initiatives and the complexity of the environment make coordinating and integrating these efforts a significant challenge. Clearly, they must fit together, complement each other, not be redundant, nor conflict with or undermine one another. Until recently, however, no unifying national approach for assuring this was in place. However, recent Executive Orders and new legislation – i.e., Executive Order 13356, the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) – provide the mandate to coordinate these efforts into an integrated and effective national strategy.

1.2.8 IRTPA Provides Needed Structure for National Information Sharing Environment

On December 7, 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), which included many of the recommendations from the 9/11 Commission and incorporated provisions from the President's Executive Order 13356.[5] This new legislation sets out new requirements, mandates, and provisions for creation of an "Information Sharing Environment" (ISE). The new ISE will provide the national policy framework, overarching

[5] This E.O. directs federal agencies, to the maximum extent consistent with applicable law, to give the highest priority in their design and use of information systems and dissemination of information to the:

- detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America;
- interchange of terrorism information among agencies; and
- interchange of terrorism information between agencies and appropriate authorities of States and local governments, and the protection of the ability of agencies to acquire such additional information.

strategy and technical interoperability critically needed to unify sharing approaches, coordinate initiatives and address the longstanding and emerging challenges that have impeded information sharing in the past.

Included in the legislation was the creation of the Information Sharing Council and a Program Manager to plan for, oversee implementation of, and manage the ISE. Under this new legislation, the Program Manager, in consultation with the Information Sharing Counsel, will develop and implement policies, procedures, guidelines, rules, and standards that address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense (DOD), the homeland security community, and the law enforcement community. The IRTPA outlines one of the primary missions of the National Counterterrorism Center, which will be to conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence, homeland security, and law enforcement activities within and among agencies.

1.3 How LEISP Fits with IRTPA and the ISE

The primary[6] focus of IRTPA is the sharing of intelligence or terrorism information as opposed to the broad spectrum of law enforcement information. Despite its critical importance, terrorism information sharing reform does not address the broader areas of more traditional law enforcement information sharing. This category of information sharing is vital to solving other crimes essential to the protection of Americans, such as serial murder, serial sexual assault, organized crime, and Internet identity theft. In many cases, traditional federal, state, local, and tribal criminal activity information may contain links to terrorism that are deeply hidden and remain outside the direct scope of terrorism intelligence.

This is where LEISP makes its contribution. LEISP fits into the Act by focusing on the broader sharing of law enforcement information. LEISP is the Department's strategy for sharing DOJ information – from all of its components – with the Information Sharing Environment created by the IRTPA. The LEISP strategy contributes to the fulfillment of the ISE by providing a single point of contact for DOJ information and by providing a foundation for information sharing among law enforcement at the federal, state, local, and tribal levels.

LEISP provides powerful support for terrorism information sharing by establishing, through its OneDOJ initiative, uniform DOJ policies and processes for sharing its information. It also will provide a foundation for broadening the reach of the ISE to the thousands of state, local, and tribal law enforcement partners, where the process of transforming data to information and finally to intelligence is most critical.

Moreover, LEISP contributes to the goals of IRTPA by enhancing the type and quantity of information that can be shared among law enforcement. This will not only benefit law

[6] While IRTPA does include in its purview the sharing of non-classified law enforcement information, reforming intelligence efforts and facilitating the sharing of intelligence information to prevent terrorism are the overarching goals.

enforcement efforts but will also contribute to the quality of intelligence in the long run. While law enforcement information is useful in its own right to detect, investigate, and prosecute criminal activities, it can also be a key input to critical intelligence and counterterrorism information. Simply put, the more law enforcement information is shared the better our intelligence capability is likely to be. This concept is clarified by examining the conversion of data into information – and information into intelligence – as discussed below.

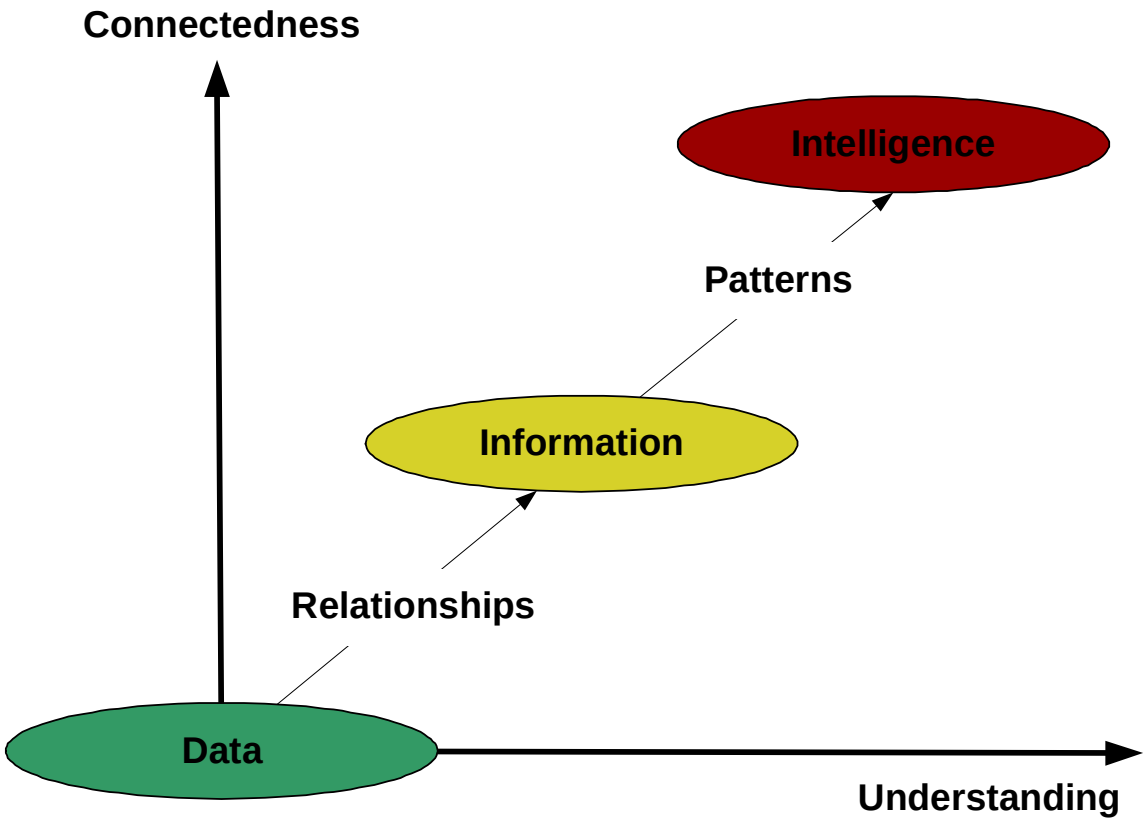
1.3.1 Data to Information to Intelligence to Action

Data, in its most fundamental form, is a series of unconnected facts. But data alone is not actionable. Data requires context in order to have any meaning. Bits of data, when collected and assembled in context, become more useful (e.g., the name in a record with an address connected to it). When connected data has specific meaning or shows a relationship, it transcends into information. When bits of seemingly unrelated information are linked and pieced together they can show a larger picture or pattern. These data and information patterns become intelligence, which decision makers use when deciding appropriate actions.

The more data that is available the more information there is that can be examined and analyzed, yielding better intelligence. Better information contributes to better intelligence. While some law enforcement information ultimately may lead to criminal intelligence or even become critical counterterrorism intelligence, there is often no way to know in advance which bits of information, when pieced together, will allow officials to connect the dots and see the larger picture that ultimately leads to the successful pursuit and prevention of criminal activities and terrorism. Therefore, it is important not to have limitations on the flow of law enforcement data and information across all jurisdictions.

The diagram below depicts the relationship between the quantities of data shared – or connectedness – and its usefulness or meaning.

Figure 1-3: Data Context and Meaning



Efforts to improve sharing of existing and future *intelligence* information will enhance our ability to prevent terrorism, but significant improvement in our overall intelligence capability and counterterrorism efforts also can be obtained by connecting and making available the vast majority of related unclassified law enforcement data and information[7] that has never been fully utilized in the past.

In other words, improving law enforcement information sharing will provide a broad policy and strategic foundation for the information sharing environment, increase the inputs to our intelligence gathering and become one of the best ways to support actionable counterterrorism efforts. Doing so is the core responsibility and capability of DOJ and the focus of LEISP. This singular focus on law enforcement information and processes distinguishes LEISP from other information sharing initiatives and provides its valuable contribution to the ISE.

[7] It is important to note that law enforcement agencies at all levels have recently begun to develop their own intelligence through such methods as fusion centers, which combine information and analysis, and regional information centers, which share law enforcement information with all law enforcement-related agencies within a region. Enhancing law enforcement information sharing through LEISP would also make this law enforcement intelligence available to the counterterrorism and intelligence communities.

1.4 LEISP: A New Information Sharing Paradigm

On May 14, 2004, DOJ joined with the International Association of Chiefs of Police, the Global Justice Information Sharing Initiative (Global) Intelligence Working Group (GIWG), and other local law enforcement organizations to endorse the National Criminal Intelligence Sharing Plan (NCISP). This plan, developed by the law enforcement community, is an important driver of the LEISP strategy because it clearly articulates the need for a comprehensive national approach for law enforcement information sharing. LEISP is DOJ's contribution to the implementation of the recommendations detailed in NCISP.[8]

As DOJ participated in the development of the NCISP, it also began to conduct a diagnosis of its own policies, processes and approach to technology related to law enforcement information exchange. This process identified the prerequisites for LEISP success. First, it will require a new paradigm for information sharing, with new policies, practices, and capabilities for connectivity among sharing partners. It will also require moving the current need-to-know culture more towards a need-to-share culture where the data-to-information-to-intelligence progression is handled in a manner that facilitates the ability to share.

This new paradigm will include new services that maximize the value that can be extracted from law enforcement data and information as well as new capabilities to efficiently and effectively share that value with appropriate partners as a matter of routine rather than exception.

LEISP is pursuing the following as critical to its success:

- LEISP is the single, coordinated law enforcement data and information sharing initiative for the entire Department of Justice. All DOJ component information sharing initiatives will be consistent with and support implementation of the LEISP strategy.
- Focus and emphasis shall be placed on law enforcement information needs and on the policies and processes necessary to address those needs rather than focusing on technology, which should be considered after business requirements are defined.
- DOJ is committed to meaningful and effective collaboration with its partners from the law enforcement community; the LEISP strategy reflects and accommodates the diverse nature of local law enforcement and unforeseen incompatibilities are avoided.
- DOJ is committed to the principle of leveraging existing and planned local and state investments and resources rather than requiring new expenditures, and will guide implementation choices to make the maximum use of current and planned investments in systems and related information sharing efforts of its partners.
- DOJ recognizes the serious constraints of local and state budgets and is committed to minimizing the budget impact to state and local authorities in every possible manner.
- DOJ, through LEISP, is committed to partnering with its federal partners, like the Department of Homeland Security, in information sharing efforts and initiatives.
- DOJ is, as a first priority, addressing its own internal barriers to information sharing and "putting its own house in order" to maintain and ensure accountability and data integrity internally and to be an effective, trusted partner for solving the information sharing

[8] To access, see http://it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf.

problems throughout the wider law enforcement community. This means the LEISP strategy is placing a high priority on implementing uniform internal sharing policies, business processes, and an integrated technology architecture, and is coordinating these with existing DOJ sharing-technology initiatives, such as the National Data Exchange (N-DEx), the Regional Data Exchange (R-DEx), Law Enforcement Online (LEO), and the Regional Information Sharing System (RISS).

- DOJ will implement LEISP along three tracks (which will overlap significantly on an implementation timeline): Track I is the implementation of OneDOJ. Track II will first incorporate "quick hits" to leverage existing sharing technology capabilities and then center on building out the technology platforms and services to enable the Department to seamlessly share its information. In Track III, the Department will work cooperatively with its federal, state, local, and tribal law enforcement partners to build the interconnectivity that will allow standard, routine information sharing across all jurisdictions on a national basis.
- DOJ's plan for improved information sharing must begin with a future vision, commitments, and principles to guide its implementation. It must delineate policies that create the conditions of trust, security, accountability, and partnership that are necessary to obtain meaningful participation by LEISP partners. It must identify the functional requirements needed for extracting value from information that is shared and point the way to a technology architecture that is acceptable and supportable to the diverse interests within the law enforcement community.

To be effective, the LEISP strategy must specifically address the challenges to information sharing detailed in the section above. LEISP does this by proposing a unified policy framework and coordinated program to address current barriers, and it creates the needed conditions to facilitate multi-jurisdictional sharing of law enforcement information.

LEISP provides a program to utilize existing and planned systems to provide needed connectivity. In addition, it sets out a forum for collaboration across the law enforcement community to develop a workable, effective approach to nationwide interchangeable data in regard to information sharing.

To help unify and coordinate the multitude of agencies across law enforcement, the strategy calls for a partnership approach to decision making and provides a forum for collaboration among information sharing partners on key issues. To address the legacy of mistrust that hangs over efforts to share information, LEISP calls for DOJ to establish a common policy framework such that those who share its information can trust that their concerns about its use will be addressed.

While the LEISP strategy envisions enhancement of trust between institutions, it also recognizes the benefit and power that existing individual trust relationships can bring to information sharing. Therefore, the LEISP strategy encourages the development of regional information sharing centers and seeks to leverage existing trust-based relationships to improve regional information sharing.

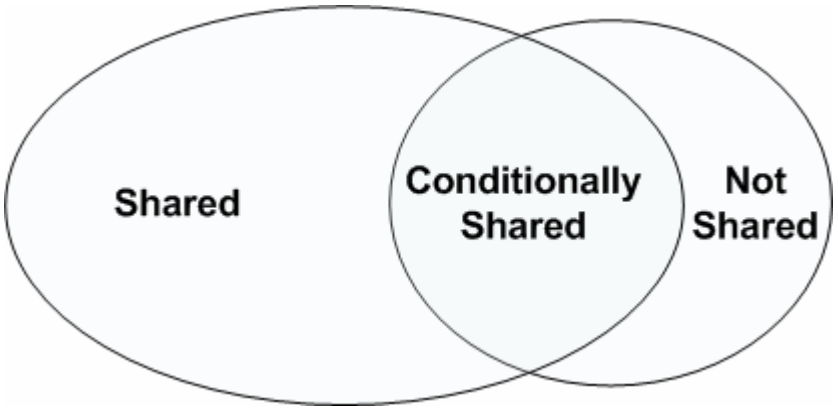
In response to the law enforcement need for better information to deal with increasingly sophisticated criminals and terrorists, LEISP provides for the creation of new capabilities and information services that will help uncover patterns of behavior and connect the dots.

To deal with the issue of categorization of information, LEISP calls for increased use of tearlines to provide unclassified versions of documents to release, as well as the development of procedures which allow information to be more accurately categorized from the beginning of collection.

The LEISP strategy seeks to create the capability for all shareable or conditionally shareable information to be shared as appropriate with LEISP partners. Achieving this will require instituting the processes and procedures necessary to more appropriately categorize information so that shareable information resides in shareable categories and systems. There will need to be strict procedures for identifying information that is not shareable under any conditions.

LEISP will also require developing policies, processes, and procedures that encompass the circumstances which allow sharing to conditionally proceed. Finally, it will require commitments by all LEISP partners to share information defined as shareable by adherence to written policies, standards, and protocols for information sharing. These actions, once implemented, would move the categorization of information model from that depicted in Figure 1-2 to that depicted in the figure below:

Figure 1-4: Target State for Information Sharing Categories

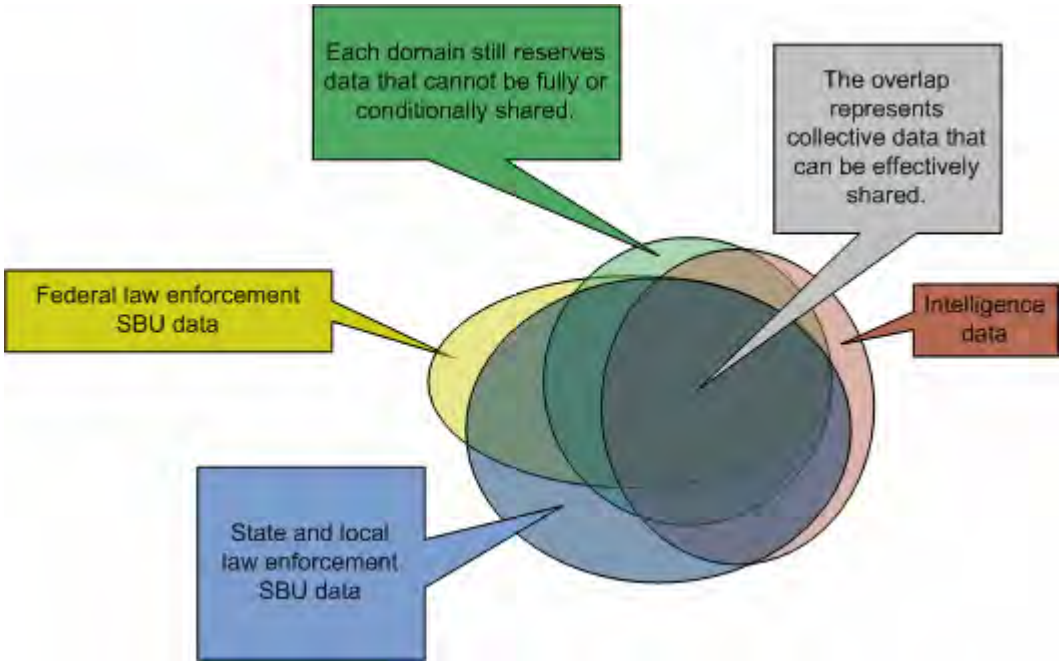


With this background, and through the LEISP strategy, DOJ seeks to initiate a forum to improve law enforcement information sharing in the United States.

The Department looks towards a collaborative effort where all interests work together to accomplish this goal, with a process that is respectful and responsive to the different needs of each member of the law enforcement community. The Department of Justice acknowledges the challenges, but sees the potential for solving the problems and overcoming the obstacles that in the past have prevented such a framework from evolving.

The implementation of the new information sharing paradigm as envisioned in the LEISP strategy would move the information sharing model to look as depicted in Figure 1-5:

Figure 1-5: Future "To Be" State of Law Enforcement Information Sharing



The following chapters provide detail of the LEISP strategy, identifying vision and commitments, guiding principles, policies, data and functional requirements, technology architecture, and an implementation approach that is committed to partnership, collaboration, and demonstration of the Department's commitment to information sharing through its efforts to implement OneDOJ.

2. LEISP Vision and Commitments

The LEISP strategy enables a vision where accurate and timely law enforcement information is seamlessly shared across jurisdictional boundaries to enhance America's ability to deter and prosecute criminal activities and terrorism. The LEISP vision is for a future where law enforcement will be able to:

- access all shareable DOJ information as standard operating procedure through a Department-wide integrated technology architecture;
- deploy powerful new capabilities to search, analyze, and disseminate data, investigative information, and intelligence from across the entire law enforcement community;
- spend more time transforming information into knowledge and less time in finding and requesting data/information; and
- routinely share information across the entire law enforcement community because of cooperatively developed standards, processes, and practices for ensuring privacy, security, and accountability.

The LEISP strategy is not a plan for a system but rather for a program that identifies the requirements, policies, and practices to achieve this vision.

LEISP is DOJ's commitment to:

- ensure DOJ information is shared comprehensively and routinely within DOJ and with other federal, state, tribal, and local law enforcement partners;
- ensure DOJ information sharing supports the requirements and needs of law enforcement decision makers from the President to the patrol officer; and
- take responsibility for making DOJ law enforcement information useful to decision makers, in formats and mechanisms that meet their needs.

To achieve these goals, DOJ will foster a forum where law enforcement from across federal, state, local, and tribal governments can come together and work cooperatively to develop requirements for integrated services that support law enforcement information sharing.

3. Guiding Principles and Policies

Guiding principles drive policies that represent the backbone of the LEISP strategy for achieving the Department's information sharing vision and commitments. The following sections articulate the guiding principles that will inform and shape decision making as the LEISP strategy is implemented and set forth the specifics of associated policies.

The first three principles and policies compose the core of what the Department is terming "OneDOJ", the Department's internal initiative to get its own information sharing house in order – a prerequisite to partnering with law enforcement agencies outside the department on improving their information sharing efforts. The remainder of the principles and policies focus on protecting privacy and establishing an environment of partnership and trust that will be critical to the creation of a national information sharing capability.

3.1. All DOJ Components Will Share Information as Standard Operating Procedure

3.1.1. Information Sharing Guiding Principle

DOJ will share law enforcement information in its possession, including tearlines of classified information, routinely with all law enforcement partners, with the exception of certain categories of information identified by the Deputy Attorney General as those that may possibly not be shared. Examples include the following:

- espionage and public corruption case information;
- information whose dissemination is prohibited under international or inter-agency agreements;
- information that would reveal sensitive undercover operations or sources and methods of information collection; and
- civil rights investigations involving color of law violations, internal investigations, and administrative cases.

In addition to establishing clear policies on information sharing, DOJ will:

- improve information sharing within the federal law enforcement community by establishing appropriate connections between DOJ and other federal information sharing systems as well as participating in regional sharing initiatives;
- create tearline unclassified versions of DOJ classified information that can be disseminated to other law enforcement agency (LEA) partners; and
- empower and enable DOJ components to share information with law enforcement partners at the local level, consistent with overall written DOJ policy and Memoranda of Understanding.

3.1.2. DOJ Information Sharing Policies

1. Information held by the DOJ will be electronically shared with federal, state, local, and tribal law enforcement, with the exception of those possible categories specified above (see Guiding Principle 3.1.1.). Information not explicitly excluded shall be shared in accord with Memoranda of Understanding (MOUs) with partners.

2. The standards for exclusion are information specific to:
   i. public corruption
   ii. sources and methods involved in collection of information
   iii. civil rights investigations involving color of law violations
   iv. internal agency or administrative matters
   v. case/investigative management decision
   vi. information the dissemination of which would violate privacy law, regulation or written policy
   vii. exclusions prescribed in existing interagency MOUs

3.1.2.2. Tearline Policy

DOJ will create tearline versions of classified information that can be electronically disseminated to federal, state, local, and tribal law enforcement. By tearline, the Department means disassociating the sources and methods of classified information from the information itself, and making the underlying information available for sharing.

3.2. DOJ Will Present All Department Components as a Single Information Sharing Entity

3.2.1. OneDOJ Guiding Principle

Under this guiding principle, DOJ will share information among its components and present itself to law enforcement partners as a single entity for information exchange. To comply with this principle, DOJ will:

- operate within a unified framework of Department-wide information sharing policies (see Guiding Principle 3.1.1) and business processes and a single technology architecture;
- coordinate and reconcile its existing and planned information sharing investments to prevent functional and technical duplication and enhance performance;
- deploy a single online point of access to shareable Department information;[9] and
- develop new capabilities and a consolidated interface where information can be shared and analyzed across multiple jurisdictions and where law enforcement partners can electronically collaborate to deter and prosecute crimes, including terrorism.

Taken together, these internal initiatives will position DOJ as a committed participant in a national law enforcement network of comprehensive, cross-jurisdictional information sharing.

[9] Point of Access may be multivariate in nature: some partners may choose to access OneDOJ via a Web portal, where others may wish to bind to a standardized application or Web interface specification. At its most rudimentary, this principle will not preclude information sharing via hard copy files.

3.2.2. OneDOJ Policy

One of LEISP's principal objectives is to ensure that DOJ information will be made available to law enforcement users at all levels of government and that all information that is part of the strategy will adhere to organizational policies concerning individual rights to privacy and operational procedures. To achieve its mission in presenting a powerful resource to the vast scope of law enforcement it serves, DOJ will present the OneDOJ initiative as a single information sharing entity to federal, state, local, and tribal law enforcement through a single, Department-wide technology architecture.

3.3. DOJ Will Protect Privacy and Ensure Security in Implementing LEISP

3.3.1. Privacy Guiding Principle

DOJ will adopt Department-wide policies and procedures to protect the privacy of individuals and the security of information it shares. This includes audit trails and sanctions, in order to maintain the integrity of information and to ensure against unauthorized access, use, and disclosure, and to assure the accuracy, completeness, timeliness and relevancy of information.

3.3.2. Privacy Policy

1. DOJ will protect the privacy of individuals by assuring that individually identifiable information shared by the Department is not misused or inappropriately disclosed.
2. DOJ will limit the sharing of information to the fulfillment of a stated law enforcement purpose (i.e., for the identification and pursuit of suspected criminals, to bring offenders to trial or to protect the safety of law enforcement officers).
3. DOJ will ensure that information shared by the Department complies with data quality and security policies.
4. DOJ will protect personal information against unauthorized access, destruction, use, modification, or disclosure, including maintaining a record of the identity of the agency and person accessing and disseminating the information in accordance with the Privacy Act's accounting provisions.
5. DOJ will publicize policies and procedures for protecting privacy of information that is shared.
6. DOJ will train its employees on privacy protection requirements and conduct periodic privacy and security audits.
7. DOJ will ensure that the privacy provisions of applicable federal laws and regulations are implemented and enforced.

3.3.3. Information Definition Policy

To meet certain requirements of the Privacy Act and other laws, the Department is required to define the kind of information that will be shared as a result of the LEISP strategy.

LEISP will allow U.S. law enforcement agencies to use computer-based systems to: (1) search and retrieve; (2) aggregate and analyze; and (3) disseminate to other authorized law enforcement officials information compiled by duly authorized law enforcement agencies related to criminal activities and terrorism.

The information capabilities will be used to investigate criminal activities that have occurred, bring into custody a confirmed fugitive and thwart criminal acts that may be attempted. The types of information that will be used, as described above, will include:

1. identifying information about individual criminal offenders or alleged offenders (e.g., name, birthdate, birthplace, physical description, address, fingerprints, DNA, or other approved biometrics)
2. criminal history information about individuals (e.g., history of arrests, the nature and disposition of criminal charges, sentencing, confinement, release and parole, and probation status)
3. criminal event data (e.g., characteristics of criminal activities and incidents that identify links or patterns)
4. criminal investigation information derived from sources, such as witness interviews, investigation reports, and surveillance reports

3.4. DOJ and Its Partners Will Establish Trust Through Organizational Accountability

3.4.1. Organizational Accountability Guiding Principle

An essential element for successful interagency partnership, for both trust and practical implementation, is organizational accountability. Under this principle, the Department will use Memoranda of Understanding to document what has been agreed to between DOJ and its information sharing partners, including standards and controls that address access to each partner's data.

From a practical perspective, responsibility for enforcing cooperatively developed rules, roles, and duties will be delegated to each partner. The community of agencies and individuals involved is far too great for the centralized administration of procedures and activities, such as vetting and authenticating authorized users, conversion of shareable data into standard formats, or monitoring agency compliance with sharing policies.

3.4.2. Organizational Accountability Policies

DOJ will work cooperatively with its partners to develop tools and processes to allow for validation of organizational accountability, including an audit function and the application of sanctions if a participating agency fails to meet its agreed-to obligations.

In developing these communitywide policies, DOJ will work with groups like the Global Advisory Committee and the CJIS APB to build policies based on accepted and trusted law enforcement community norms of operation, such as:

- Partner Commitment to Information Sharing: to state that all partners have an obligation to share information unless specifically prohibited by law, regulation, or written policy (see Guiding Principle 3.1.1.).
- Privacy: to ensure that the maintenance and exchanges of shareable information complies with applicable privacy standards and legal requirements.

- Memoranda of Understanding: to document the rules, roles, practices, procedures, and responsibilities to which each partner is committed.
- Partner Preparedness: to identify and support the preparedness of partners that share information with DOJ.
- Ownership, Entry, and Maintenance of Information: to ensure that ownership of information made available for sharing remains with the organization that originated the data and that such data cannot be distributed to others without the permission of the owner.
- Quality Assurance and Quality Control: to establish the data quality responsibilities of each partner agency that makes information available for sharing.
- Auditing: to establish a communitywide and partner-specific audit capability and associated sanctions for non-compliance with mutually agreed-upon policies.
- Security: to identify the common security controls that partners are responsible for implementing and maintaining.
- Vetting: to identify the responsibilities that each partner has for authenticating the identity of users and authorizing information shared under MOUs.
- Technical Standards: to guide each partner in its data sharing with other partners, while seeking to minimize development and maintenance costs of integration and maximize the potential of local and internal resources through standardization and reuse of universal components.
- Training: to establish partner responsibilities for training their employees who access information obtained under the Memoranda of Understanding.

3.5. DOJ Will Participate In Local and Regional Sharing Initiatives

This guiding principle commits DOJ to contributing to the success of existing trust-based relationships in the law enforcement community by participating in multi-jurisdictional sharing initiatives; however, it does not have an associated policy but rather calls for standards development.

DOJ will develop internal standards and a structured process for determining how to most effectively participate in local and/or regional information sharing initiatives that bring together federal, state, local, and tribal law enforcement agencies.

The Department will rely heavily on the CJIS APB collaboration model and the cooperative environment envisioned by Global and the NCISP in developing these standards, including standard formats for Memoranda of Understanding, which may be established on a statewide basis, regionally, or on an agency-by-agency basis.

Examples of areas where standards are envisioned include:

- standards for data definitions, data structure (GJXDD & GJXDM)
- security and federated trust models
- law enforcement roles and privileges models
- electronic data messaging formats and protocols
- law enforcement business practices

- law enforcement information services
- data service interfaces

The guiding principles and policies of LEISP articulated above provide direction and context for the data requirements and functional requirements of effective law enforcement information sharing discussed in sections 4 and 5, respectively.

4. Data Requirements for Law Enforcement Activities

Law enforcement has different activities and operational capabilities that have varying needs for information, different data collection sources, and, in turn, a variety of information sharing formats and mechanisms. DOJ information sharing will support the needs of law enforcement decision makers by ensuring that information sharing functions and services address the needs and sources for all the different activities.

4.1. Information Needs by Operational Capability

Law enforcement has, in general, three operational capabilities that require information sharing: tactical, investigative, and analysis. Each of the operational capabilities requires specific information and has different demands for information sharing.

4.1.1. Tactical

Officers and agents need tactical information on the status of individuals, vehicles, or incidents to make decisions on the threat a person or situation represents or if a legal basis exists to question an individual, make an arrest, or conduct a search.

Information supporting a tactical need must be readily and easily available, accessible within a short period of time (i.e., seconds), and actionable without a requirement to validate the information or its source.

The sources of data supporting the tactical situation may be limited (i.e., the information passed to the requesting officer is not everything law enforcement knows), but the sources are reliable, relevant, and legally appropriate. In general, information supporting the tactical function needs to be available to anyone performing authorized duties.

4.1.2. Investigative

Investigative law enforcement is the methodical examination of a criminal event and/or an individual or organization suspected of committing or planning a criminal act. Agents performing investigative functions require detailed information on people, places, things, and events.

Law enforcement also may need to know who else is investigating the suspect(s) or incident(s) in question. Information supporting an investigative need does not always need to be available or accessible within a short period of time. In addition, information may not be actionable without further validation.

Information needed for investigations tends to be more comprehensive than tactical information, but it still may represent only a subset of what law enforcement knows. The investigator will need to validate and coordinate the relevance of the information and legal appropriateness of using the information to justify action or sharing the information with another law enforcement

agency. In general, only law enforcement personnel conducting investigations will have access to the information designed to fulfill specific investigative needs.

4.1.3. Analysis

Law enforcement agencies at all levels have recognized the need for good analysis capabilities, and most states and major cities have established such operations. Currently, analysis functions vary widely across the law enforcement community. Nonetheless, almost all law enforcement agencies need to develop knowledge about ongoing and potential criminal activity and to provide analyzed information for command and control purposes.

Law enforcement analysis supports and informs all law enforcement operations. It uses a number of different processes to create knowledge and understanding from disparate information obtained from a variety of sources, some of which are not readily available or accessible within short periods of time.

Analysis requires access to data from agency records systems, reports from patrol officers and field agents, and intelligence products of other intelligence organizations. Analysis personnel also require tools to manage and analyze data, and need to be able to provide the results of analysis to agents/investigators working cases, agency command, and intelligence organizations.

To support command-and-control and law enforcement managers, analysis also requires information on the scope of criminal activity in their jurisdiction (to support resource and budget requests/allocations) as well as nearby jurisdictions that could impact their operations. Effective jurisdictional leadership requires the ability to issue commands to their agents/officers and alerts/notifications (e.g., all-points bulletins, requests for assistance) to other law enforcement agencies and others outside the law enforcement community (e.g., first responders). Such leaders also need an ability to exchange strategic intelligence with peers from other jurisdictions (e.g., task force operations).

4.2. Information Needs by Activity

The following subsections describe more specific information sharing requirements for core tactical and investigative law enforcement activities, as well as analysis (including support for command and control functions).

To fulfill their objectives, law enforcement agencies conduct a number of activities to detect and investigate terrorist and criminal activity, including:

- patrol/traffic enforcement
- arrest/apprehension
- emergency response/incident management
- surveillance
- case specific investigation
- task force investigation

These core law enforcement activities are facilitated and influenced by investigative and analysis functions and managed through some form of a command and control function.

4.2.1. Patrol/Traffic Enforcement

The most common contact the public has with law enforcement is interaction with patrol officers through traffic stops. These contacts often yield a wealth of information for criminal investigation and prevention purposes.

Although DOJ has limited patrol functions, other federal agencies (e.g., Park Police, Customs and Border Protection, DOD, and the Transportation Security Administration) have extensive patrol or related security functions. In addition, DOJ investigations rely on assistance from state and local law enforcement patrol functions to help collect information and identify the location of fugitives or suspects.

Patrol officers need several types of information to execute their routine responsibilities, to assist investigators, and to maintain their personal safety. They need access to information on wanted persons and stolen vehicles. They also need the ability to quickly and positively identify persons. To assist investigators or intelligence functions, they also need to know "who or what to be on the lookout for."

Patrol officers/agents typically are provided information in one of four situations: pre-patrol briefings, notices or alerts while on patrol, as a result of queries they submit while conducting a stop (e.g. traffic, suspicious person), or in making an arrest. They also collect and report information to command authorities, investigators, and potentially to officers of another agency.

Information may be collected by patrol officers as a result of specific requests from others or self-initiated based on a suspicion of criminal activity, intuition, knowledge, or training. Information collected by patrol officers typically is documented in field interviews or suspicious person reports, preliminary criminal offense reports, or traffic citations.

4.2.2. Arrest/Apprehension

Arrest or apprehension of suspects or fugitives is a common duty performed by many law enforcement officials. During apprehensions, officers need access to information about the person(s) being apprehended (e.g., identity, location, armed and dangerous, associates). They also should know if other law enforcement agencies are seeking or investigating the same individual(s).

Officers engaged in apprehensions typically receive information during operational briefings (e.g., if the apprehension is planned), in response to a query (e.g., if the apprehension is based on a traffic stop or observance of a crime), or on tips from the public.

At the time of arrest, officers report the apprehension and information about the person and circumstances of the arrest to appropriate supervisors and other persons.

4.2.3. Emergency Response and Incident Management

Officers are dispatched to respond to a wide variety of incidents, including to the scene of homicides, robberies in progress, the discovery of a bomb or an explosion, or a hostage situation. In such circumstances, officers need to know details on the incident, identities or descriptions of individuals involved, specific information about the incident scene (e.g., the type of explosive

device found), other agencies involved, and, in some cases, an ability to reach out for the expertise of another agency.

The timing of an incident is never planned so officers receive information about the incident as part of instructions to or as a result of queries or requests while executing their duties at the scene. In the event of large-scale incidents and emergency response, command posts can be established, through which additional information is generated and disseminated. Typically, the type and amount of information needed by responding personnel is the same regardless of whether a criminal incident, a suspicious incident later found to be criminal, or a suspicious incident later determined to be non-criminal has occurred.

Information on the circumstances of the incident and people involved is reported by the responding officer to appropriate supervisors and other persons.

4.2.4. Surveillance

Officers also are called upon to conduct surveillance to collect information as part of an ongoing investigation or to deter a criminal action. Surveillance is typically focused on observations of individuals, locations, businesses, or motor vehicles.

Officers performing surveillance require information about likely locations, habits/actions, means of transport, associates, whether a person is armed and dangerous, and whether other law enforcement agencies have an interest in suspects. If surveillance is conducted as part of an ongoing investigation, they also will likely need to know the details of the case.

Information needed to support surveillance is typically acquired through access to case records, briefings, or responses to queries made while conducting the surveillance. Officers likely will report information collected during surveillance through their command structure.

4.2.5. Case Specific Investigations

Upon discovery of a crime, or while investigating a tip and/or report about a crime, investigators collect information about subjects and events related to the case.

Investigators seek information from a range of sources, depending on the specifics of the case. Included are agency's records, case files, record systems and case files of other jurisdictions, consolidated records systems (e.g., NCIC), specialized databases, and public source data.

As investigators identify suspects, locations, motor vehicles, or other items of interest, they reach out to other law enforcement agencies that may have similar investigative interests or contacts. Unlike tactical operatives, investigators also attempt to analyze or connect disparate pieces of information to develop conclusions.

Most of the information investigators collect comes in response to queries or by information received from an intelligence analyst, another investigator, or a patrol officer who knows of the investigator's interest or information gleaned from an unrelated activity (e.g., traffic stop, arrest on other charges). Investigators also may obtain information from performing advanced analysis on data obtained during the investigation.

Investigators report information collected or the results of analysis through their command structure.

4.2.6. Task Force Investigations

Task force investigations are similar to other criminal case investigations except for the fact that they typically focus on a series of crimes or a type of criminal activity (e.g., organized crime, terrorism, drug cartels, gangs). They also often deal with a very sensitive or high-profile investigation (e.g., public corruption).

Task forces typically involve multiple agencies and jurisdictions. Consequently, the need to exchange information across agencies or jurisdictions is a fundamental requirement. As a result, task forces rely on information from agents and agencies outside of those participating on the task force. Due to the nature of many task force investigations, information developed may be held closely in an effort to minimize compromise.

4.3. Law Enforcement Data Needs by Source

Most law enforcement agencies operate within the routine contexts of information gathered in the course of the above-listed functions. Specific documents or records of each event or incident encapsulate these events. Typical law enforcement agencies, therefore, are creating and collecting these records and documents on an hourly basis and have routine need for discovering similar historical documents within the law enforcement community to help them determine the appropriate course of action to be taken as a next step in the law enforcement cycle. The following are examples.

4.3.1. Field Information (Incident) Report (or FI)

These are typically brief reports collected about a party who may appear to be involved or related to potential criminal activity but wherein charges (or evidence necessary for arrest and detention) are not immediately pursued.

4.3.2. Traffic Citation/Accident Report

These are also relatively brief records, but specific incidents that are not assumed to be criminal in nature, or can be handled without arrest and detention of the subjects involved.

4.3.3. Incident Report/Arrest Reports

The nature of these two reports, in form and substance, are generally the same and only differ on the context of whether one or more parties of the incident are both present and placed under arrest. Both reports are predicated on probable cause of criminal activity with a presumed intent to bring formal charges against one or more of the subjects of the incident. In many cases, however, an incident may be only the report of a crime from a citizen or witness, and such an incident may not have an identified subject immediately related to the record. Therefore, the completeness of these records, comparatively on a one-to-one basis, is inconsistent depending on the nature and development of each incident over time. The patrol officer at the scene usually completes the initial incident or arrest. Further information, such as photos, diagrams or drawing of a crime scene, witness statements, or further investigative information from the on-scene patrol functions may also be attached, along with incident/arrest narrative and/or supplemental

reports. This collection of information will then be forwarded to either an investigative officer for continued case development or presented to appropriate prosecution authorities for action.

4.3.4. Warrants

As issued by the court of jurisdiction, warrants arise from law enforcement matters (such as in the case of incidents where the subject was not present, identified, or apprehended) and highlight the identification of a subject and a charge of a criminal activity. Different warrants exist (e.g., arrest warrants, bench warrants, arrest-and-detain orders, extradition warrants) with each carrying different histories on cases or status of the defendant named in warrants for a variety of reasons (e.g., failure to appear, violations of a court order)

4.3.5. Other Information Sources

In addition to the records and documents created and maintained by law enforcement, there are numerous other information sources or collections of data that are routinely leveraged. These are gathered and maintained by other non-law enforcement agencies and/or are collective sources of law enforcement data at federal or state systems. They include:

- drivers registrations/traffic history
- vehicle registrations
- criminal history records
- stolen vehicles and property
- firearms registrations
- missing persons index
- "Be On the Look-Out" (BOLO) records

As a critical strategy for law enforcement information sharing, these documents and records need to be collected and shared in a consistent manner and format. The LEISP, recognizing the common form and need of these records, seeks to leverage the design work already conducted by the state and local law enforcement community through both the SEARCH JIEM methodology and the development of the GJXDM.

The Justice Information Exchange Model (JIEM) methodology has identified the routine and standard sharing of these documents and the consistent context and business uses for each. Furthermore, efforts within the GJXDM development process are currently vetting national reference models for each of these business component documents. In other words, the SEARCH JIEM methodology introduces standard business rules for collecting and using these documents, and the GXJDM Reference Documents set national format and content standards for sharing these documents electronically.

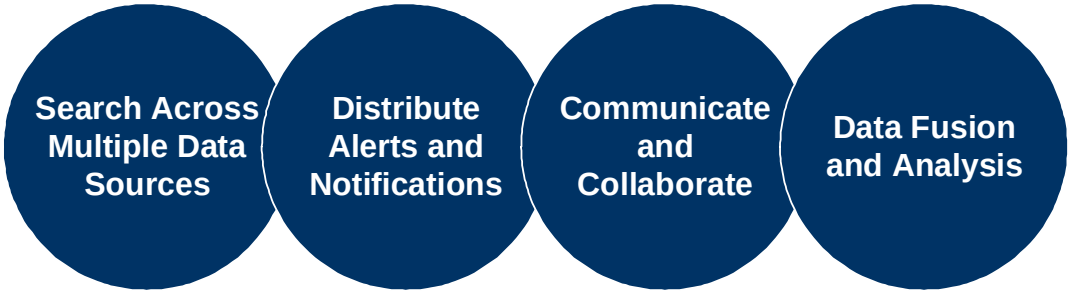
5. Functional Requirements for Information Sharing

In developing the LEISP strategy, the Department asked the following question: What are the functional requirements needed to improve DOJ's ability to meet the data requirements for law enforcement activities by sharing information with its partners and participating in a trusted network for information sharing?

As shown in Figure 5-1, law enforcement identified four functional requirement categories as critical to achieving the LEISP vision. These range from searching across multiple data sources to data fusion and analysis.

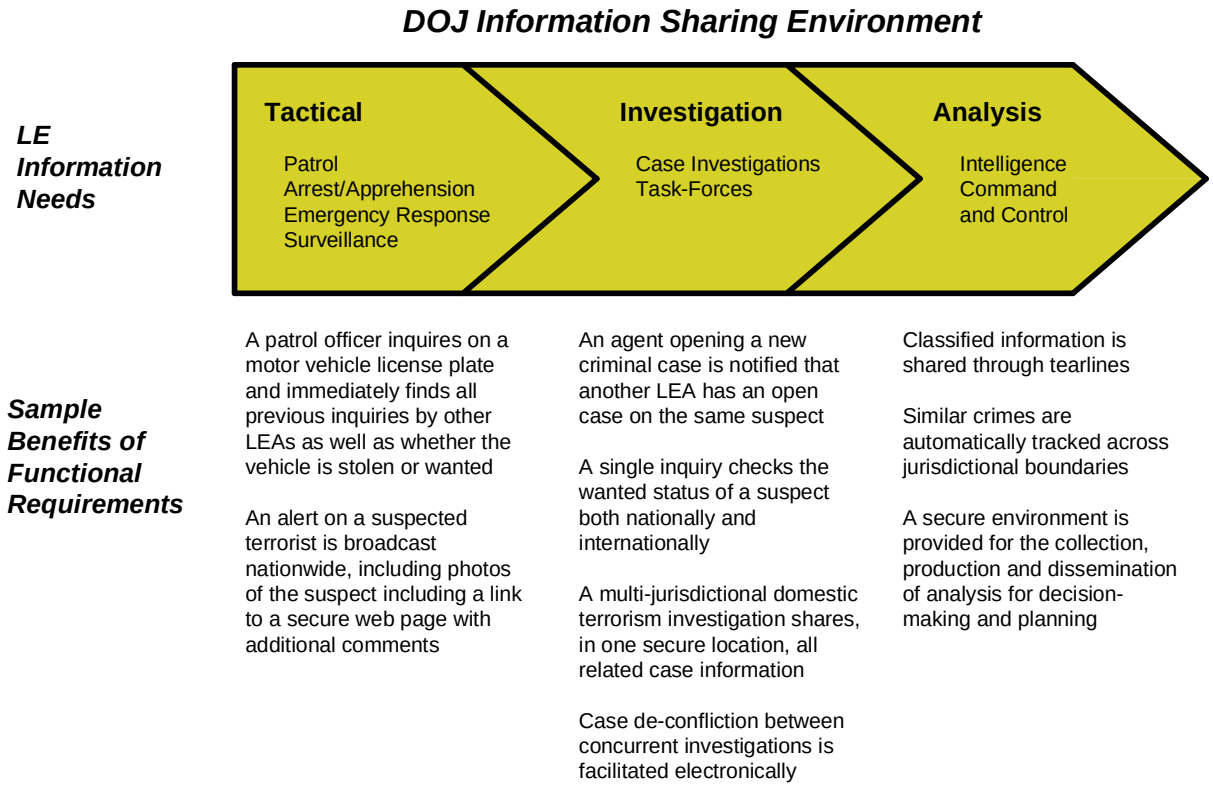
The functional requirements identified in this chapter are based upon an examination of the information needs of the respective law enforcement environments: tactical operations, investigation, and analysis.

Figure 5-1: Functional Requirement Categories for Law Enforcement Information Sharing



As per the guiding principles outlined in chapter 3, DOJ will meet these requirements by leveraging existing and planned systems to support identified information sharing needs and functions. Satisfying these functional requirements will establish the trusted network and capabilities required to support law enforcement operations. Figure 5-2 presents examples of the benefits to be provided to each environment by the identified function. More specifically, the functionalities described provide information to authorized users in a transparent, secure, trusted, and automated fashion, regardless of where the information is stored.

Figure 5-2: LEISP Functional Requirements Framework



The following sections summarize each of the functional requirements identified for law enforcement operations based upon information sharing needs.[10]

5.1. Specific Entity Inquiry

This function would provide law enforcement with a single interface (or service function) for conducting inquiries on specific identifiers (e.g., name, date of birth, and physical address) across multiple sources of information, including specific international sources (e.g., Interpol). Sources for the inquiry would be transparent to the user but would be identified in the response if a match were to be made based on the inquiry parameters.

5.2. Identity Discovery and Confirmation

This function would provide a single interface to inquire on and submit personally identifiable information, such as fingerprints or DNA data. In addition, it would provide future capabilities

[10] References in this document to the "interface" or "access" for these services is intended to be generic: in each case, it is proposed that an LEISP framework of services will be accessed by a variety of methods via a Web portal, where others may integrate these services directly into existing regional or local applications or existing network or service platforms. Others may need to access these data services by phone, fax, or paper depending on situational capabilities.

on legally accepted forms of personally identifiable information (PII) when these become available.

5.3. Multicultural Name Resolution

This function would provide tools to understand the structure, known derivations, and use of multicultural names. Queries also would be integrated into the Specific Entity Inquiry capability described in section 5.1. In addition, this function would allow a standalone lookup capability that incorporates its results into a future inquiry.

5.4. Query Transaction Index

This function would provide a historical view of law enforcement queries through a searchable index derived from the records (e.g., transaction logs) of previous information queries. These logs typically include such information as date, time, query parameters, and requestor identification. Cache services in the framework could also be set with specific business rules (i.e., the LEISP platform could send alerts when a certain subject or topic has been queried [n] instances over [x] period of time.)

5.5. Alert Notification

This function would provide a law enforcement agency with the ability to send electronic alerts to other law enforcement agencies. These alerts could be targeted by area (e.g., region, state, locality) and classified by subject (e.g., child abduction, robbery, wanted fugitive). Users would be able to create and maintain their own distribution lists for alerts, including specifying the delivery mechanism (e.g., telecommunications terminal, e-mail, mobile device).

5.6. Future Event Subscriptions

This function would provide the ability to subscribe to future events about subjects of interest (e.g., license plate and phone number) and set a notification threshold that includes parameters for matching (i.e., one or more specified data elements), type of notification requested based on a match (i.e., urgent, normal, etc.), and method of delivery (e.g., e-mail and mobile device), all through a single interface.

5.7. Case Information Correlation Subscription

This function would provide an automated mechanism for users to submit specifically identifiable information on an investigation and receive a notification when another law enforcement agency is interested in the same subject matter.

5.8. Secure E-mail

This function would allow law enforcement agencies to use current e-mail clients to send confidential communications to other law enforcement partners over current transport mechanisms, including a law enforcement directory lookup capability. It would support current e-mail capabilities, including distribution lists and attachments. It also would include a lookup service to provide an online directory for locating specific agencies and/or officers through a single interface. The directory would provide contact information for agencies and users, including originating agency identifier (ORI), name, address, title, phone, and e-mail.

5.9. Collaboration Zone

This function would provide the ability to collaborate electronically in a secure environment to share information for a specific task force or analytic effort. With this functionality, law enforcement would be able to create limited secure storage locations for the analysis and sharing of selected information specific to a particular case, task force case, or specialized analytical effort (e.g., fusion center).

5.10. Operational Decision Support

This function would provide users predefined reports that address trends in inquiries, results and other operational details. In addition, this functionality would support ad hoc inquiries. Users would be able to subscribe to information reports about activity that occurs within user-defined parameters (e.g., locality, county, region, timeframe, type of event).

5.11. Predictive Analysis

This function would compare and correlate specifically identifiable information (e.g., name, motor vehicle registration, serialized property) contained within inquiries conducted through NCIC-, NLETS-, and LEISP-enabled systems. For example, users could find out how often an inquiry on a certain license plate has been requested within a geographic area over a certain time period.

5.12. Data Fusion and Analytical Support

This function combines capabilities targeted at the collection, fusion, and analysis of information of different agencies in support of multi-agency, multi-jurisdictional investigative cooperation. This combination (or fusion) would allow the sharing of targeted information in a single repository or by interfacing among agency repositories to facilitate the application of centralized (i.e., shared) and local analytical tools.

In addition to these services, other administrative support services are required to administratively and legally support the functions specified above. The Department will ensure that its internal policies and processes are aligned with these requirements and will collaborate with its law enforcement partners to develop consistent communitywide administrative support services as DOJ extends new sharing capabilities to its partners. Administrative support services include:

5.13. Security Support

All law enforcement agencies that participate in the kind of routine information sharing envisioned by the LEISP strategy need reasonable assurance that their communications are, and will remain, secure (i.e., known and trusted environment). By making use of commonly accepted standards and technology to publish information, information sharing partners will be able to protect their information and the information obtained from other partners.

5.14. Automated Auditing Support

At the heart of a trusted resource or network is the accountability of the users. The capability to audit usage and dissemination down to the individual user and information accessed will give

partners the ability to maintain trust in the sharing environment. This will facilitate organizational accountability and allow for the validation of compliance by all partners.

5.15. Data Quality Support

A data quality support capability will be required to monitor and record information about the data attributes essential to the identified information sharing functional requirements, including format elements, accuracy elements, data generation, and reuse elements, timeliness of information submission, system availability, legal compliance, response time, reliability, comprehensiveness, and relevance. Most of the capabilities for these data quality requirements are already provided in the adoption of the GJXDM.

5.16. Information Usage Reporting

This support service functionality would provide the capability to access pre-defined reports produced at specific time intervals. Reports would include various views of information access, including ranking of service usage, geographical usage patterns, agency usage patterns, and similarly relevant reports.

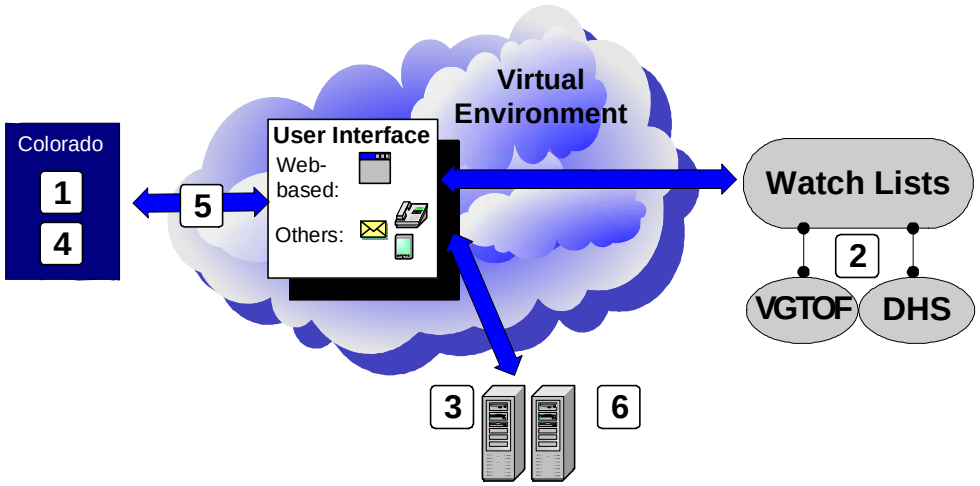
6. Operational Scenario Examples

The following example scenarios are presented to illustrate the operational benefits of the functional requirements and capabilities identified in chapter 5.

6.1. Linking Multiple Gang-Related Homicides

A local Colorado police department in a large metropolitan area is called to the scene of a fatal shooting with one victim. Investigators query the name of the victim through the Specific Entity Inquiry Service and receive a response that the victim is listed as a documented gang member in the Violent Gang Terrorist Organization File. An additional response comes from a neighboring police department as a result of a match from the Case Information Correlation Subscription Service. A call to the neighboring law enforcement agency reveals that the victim of the homicide is a suspect in a drive-by shooting two days earlier.

Figure 6-1: Linking Multiple Gang-Related Homicides



1. Local police department responds to shooting scene
2. Inquiry on victim shows an entry in VGTOF
3. Same inquiry on victim matched to case from another jurisdiction
4. Crime analyst determines homicide is in close proximity to area with increasing gang activity
5. Analysis prompts additional inquiries
6. Two additional gang-related homicides are linked to the ongoing investigation

The information is provided to a crime analyst with the first police department. The crime scene is plotted on a map of the area, indicating that the homicide location is in close proximity to an

area with increasing gang activity. Additional Specific Entity Inquiries on information from the Report of Investigation leads to the linking of two other gang-related homicides in two more cities in the metropolitan area based on evidence at the crime scenes and witness statements. As a result, the four law enforcement agencies undertake a joint investigation that focuses resources and investigative activity.

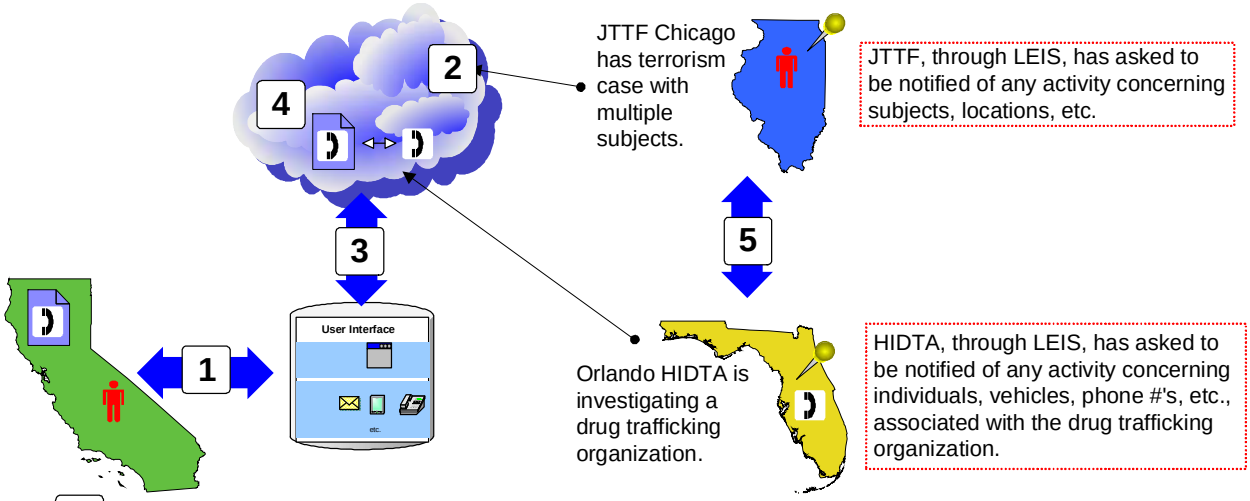
Outcomes:

- A single inquiry identifies attributes of the victim with links to an ongoing investigation in another jurisdiction
- Multiple local investigations are quickly linked, first by automated correlation then augmented by human analysis
- Previously disparate investigations are linked without human intervention, allowing for quicker de-confliction and focusing of limited investigative resources.

6.2. Drug Trafficking and Terrorism Linked Through Traffic Enforcement

The Joint Terrorism Task Force (JTTF) in Chicago has initiated a terrorism investigation with multiple subjects. Using the Future Event Subscriptions functional capability, the task force subscribes to be notified of future activity involving any of the subjects and requests that Field Interview Reports (FIRs) be completed on all subjects associated with the contact.

Figure 6-2: Drug Trafficking And Terrorism Linked Via Traffic Enforcement



1. After a traffic stop, CA Highway Patrol (CHP) conducts LEIS inquiry of vehicle and occupants.
2. CHP receives notification of Chicago JTTF subscription on one of the occupants and request to complete a Field Interview report.
3. CHP documents phone numbers on the rental car registration in the Field Interview report and submits to LEIS.
4. A phone number on rental agreement is matched against the Orlando HIDTA subscription.
5. A phone number associated with a drug trafficking organization is now linked to a subject who is being investigated by Chicago JTTF (and stopped for traffic violation in California).

The High Intensity Drug Trafficking Area (HIDTA) Task Force in Orlando, Florida, is investigating a drug-trafficking organization. The Task Force submits specific individuals, vehicles and phone numbers associated with the drug-trafficking organization to the Future Event Subscription capability.

The California Highway Patrol (CHP) conducts a traffic stop on Interstate 5. The officer conducts a Specific Entity Inquiry of the rental vehicle and both occupants. The officer is notified of the Chicago JTTF subscription on the driver of the vehicle and is informed that the JTTF is requesting the completion of an FIR on the vehicle and occupants. The Chicago JTTF receives a notification of the match by CHP.

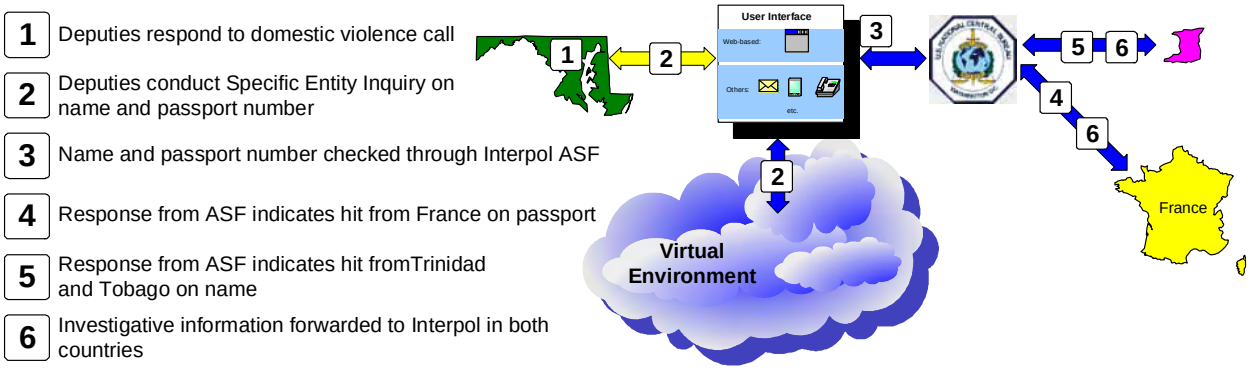
The CHP officer documents the identities of the driver and occupant, including the rental car registration and phone numbers from the agreement, on the FIR. The FIR is submitted by the end of the officer's shift into the local CHP system. The information in the FIR is then (depending upon the interface chosen by CHP to LEISP – automatically or manually) submitted to the LEISP within 24 hours. The Case Information Correlation Subscription capability matches the phone number on the car rental agreement with one of the phone numbers subscribed to by the Orlando HIDTA Task Force. The CHP officer and HIDTA Task Force agent are sent a notification of the match on the phone number.

Chicago JTTF reviews the FIR that now contains the results of the Orlando HIDTA match. The JTTF contacts the HIDTA Task Force in furtherance of the JTTF investigation. As a result of the traffic stop, JTTF Chicago documents the presence of a terrorism suspect in a new area of the country. This in turn generates new leads in the investigation. In addition, Orlando HIDTA learns that a phone number associated with a drug trafficking organization is now linked to a subject who is also linked to the JTTF Chicago terrorist investigation. As a result, Chicago JTTF and Orlando HIDTA make phone contact and work to de-conflict their concurrent investigations and collaborate on future action.

6.3. Domestic Disturbance Leads To Arrest of International Fugitive Wanted For Murder

A sheriff's office in Maryland is dispatched to the scene of a domestic disturbance near a public sporting facility. Witnesses identify two persons as involved in the disturbance. As the deputies are questioning the male and female, one of the witnesses informs the deputies that prior to their arrival the male hid a duffle bag behind a parked vehicle. The male subject refuses to identify himself, and disavows ownership of the duffle bag. Based on witness statements and physical evidence, the male subject is arrested for domestic violence. The duffle bag is searched and a foreign passport is found inside.

Figure 6-3: Domestic Disturbance Leads to Arrest of International Fugitive Wanted For Murder



The deputies conduct a Specific Entity Inquiry on the name, date of birth, and passport number. No domestic information is returned. However, the Specific Entity Inquiry also creates an additional inquiry to the Interpol Automated Search Facility (ASF).

The response from the ASF indicates the passport number is a stolen blank taken in an armored car robbery in France, where 9,000 passport blanks were taken. In addition, the name on the passport is listed as an alias on an Interpol Red Notice for murder from Trinidad and Tobago. The response provides a telephone number to call for confirmation. The United States National Central Bureau (USNCB) for Interpol is contacted and is able to retrieve the Red Notice containing a photograph of the suspect as well as the correct name.

The suspect is held on local charges pending the arrival of the Provisional Arrest request from Trinidad and Tobago. The USNCB duty agent notifies the Department of Justice Office of International Affairs and the United States Marshals Service for follow-up. The USNCB duty agent is able to retrieve interview and investigative information from the sheriff's department and forward the information to Interpol France for a follow-up investigation on the armored car robbery and to Interpol Trinidad and Tobago for a follow-up on the murder.

7. Implementation Plan

Having developed the vision and guiding principles (and having identified the information sharing needs and functional requirements for LEISP), this chapter describes the LEISP implementation roles and responsibilities, the three implementation tracks, implementation collaboration management, implementation coordination, and program management.

The LEISP implementation plan recognizes that success will depend on the Department's ability to overcome its own barriers to sharing and address the needs and requirements of federal, state, local, and tribal law enforcement partners. That is why "putting DOJ's house in order" is the first priority of the implementation plan.

As the OneDOJ goal is achieved, the Department will present itself as a single information sharing entity to its federal, state, local, and tribal law enforcement partners. Finally, DOJ will facilitate multi-directional information sharing between the Department and its law enforcement information sharing partners. Implementation will be managed through three tracks, as shown in Figure 7-1. The tracks are overlapping and not sequential.

Figure 7-1: LEISP Implementation Framework

Implementation Tracks	Track I: Achieve information sharing in DOJ (One DOJ)	Track II: Enable partner access to DOJ (one-way)	Track III: Enable multi directional sharing (two-way)
Process	DOJ internal collaboration	Collaboration with partners	Collaboration with partners
Participants	DOJ Components; DOJ OCIO; Steering Committee; JICC	State, local and other federal DOJ partners	State, local and other federal DOJ partners
Activities	Start information sharing now (link DOJ and DHS systems) Establish common information sharing policies and practices Reconcile and coordinate existing and planned information sharing initiatives Create a consolidated DOJ sharing gateway with new tools for searching, distributing, collaborating on and analyzing information	Develop technology architecture requirements for partner connectivity Develop relevant partner policies for one-way Develop funding requirements for one-way	Develop technology architecture requirements to enable partners to contribute their information to DOJ Develop relevant partners policies for two-way Develop funding requirements for two-way
Activities	DOJ as an integrated information sharing entity	Law enforcement access to DOJ sharing gateway and tools for partner use of DOJ information	National, communitywide information sharing environment

Track I will focus on integrating DOJ policies, business processes and technology necessary to present a single, uniform information exchange face to its federal, state, local, and tribal law enforcement partners.

Track II will first incorporate "quick hits" to leverage existing sharing technology capabilities and then center on building out the technology platforms and services to enable the Department to seamlessly share its information.

In Track III, the Department will work cooperatively with its federal, state, local, and tribal law enforcement partners to build the interconnectivity that will allow standard, routine information sharing across all jurisdictions on a national basis.

7.1. Implementation Roles and Responsibilities

- The Office of the Deputy Attorney General (ODAG) serves as the executive sponsor of the LEISP strategy implementation.
- LEISP implementation will be closely coordinated with and integrated into the Information Sharing Environment delineated by the Intelligence Reform and Terrorism Prevention Act of 2004, and will fall under the auspices and structures created by the Act, specifically, the Program Manager, the Information Sharing Council, and the Information Sharing Policy Coordinating Council.
- Individual DOJ components and the Office of the Chief Information Officer (OCIO) are managing specific projects within the OneDOJ track.
- An LEISP Steering Committee, the Justice Intelligence Coordinating Committee (JICC) and the Office of Information and Privacy are providing policy advice and counsel.
- DOJ's Chief Privacy Officer will provide advice and counsel in regard to LEISP-related privacy issues.
- The JICC will focus on overarching policy and information sharing requirements.
- The LEISP Steering Committee, with support from LEISP staff, will focus on ensuring that component LEISP projects are implemented consistent with the strategy.

7.2. Track 1: Achieve Information Sharing in DOJ (OneDOJ)

OneDOJ is the centerpiece of the LEISP implementation approach and will allow the Department to model the depth and breadth of sharing set forth in the LEISP vision while demonstrating its commitment to information sharing and its role as an active partner in the law enforcement community. Figure 7-2 outlines the three steps within the OneDOJ approach.

Figure 7-2: OneDOJ Approach

7.2.1. Establish Uniform Business Processes

One existing barrier to DOJ-wide information sharing is a lack of uniform information sharing business processes. Under this OneDOJ activity, the Department will develop and implement uniform policies and business processes for all DOJ components as shown in Figure 7-3.

7.2.1.1 Uniform Information Sharing Processes

Working through the Office of the Deputy Attorney General and DOJ's Joint Intelligence Coordinating Council, the Department will create uniform processes for the DOJ-specific policies detailed in chapter 3, including:

- Information Sharing Commitment: to declare DOJ's commitment to share its information with partners unless specifically prohibited by law, regulation, or written policy.
- Tearline (i.e., the ability to declassify and disseminate otherwise classified information): to declare DOJ's commitment to provide relevant national intelligence information to state, local, and tribal law enforcement in a manner that can be used by these authorities.
- DOJ as Single Information Sharing Entity: to declare that DOJ will present itself to federal, state, local, and tribal law enforcement as a single information sharing entity.
- Privacy: to ensure that the maintenance and exchanges of shareable information comply with applicable privacy standards and legal requirements.

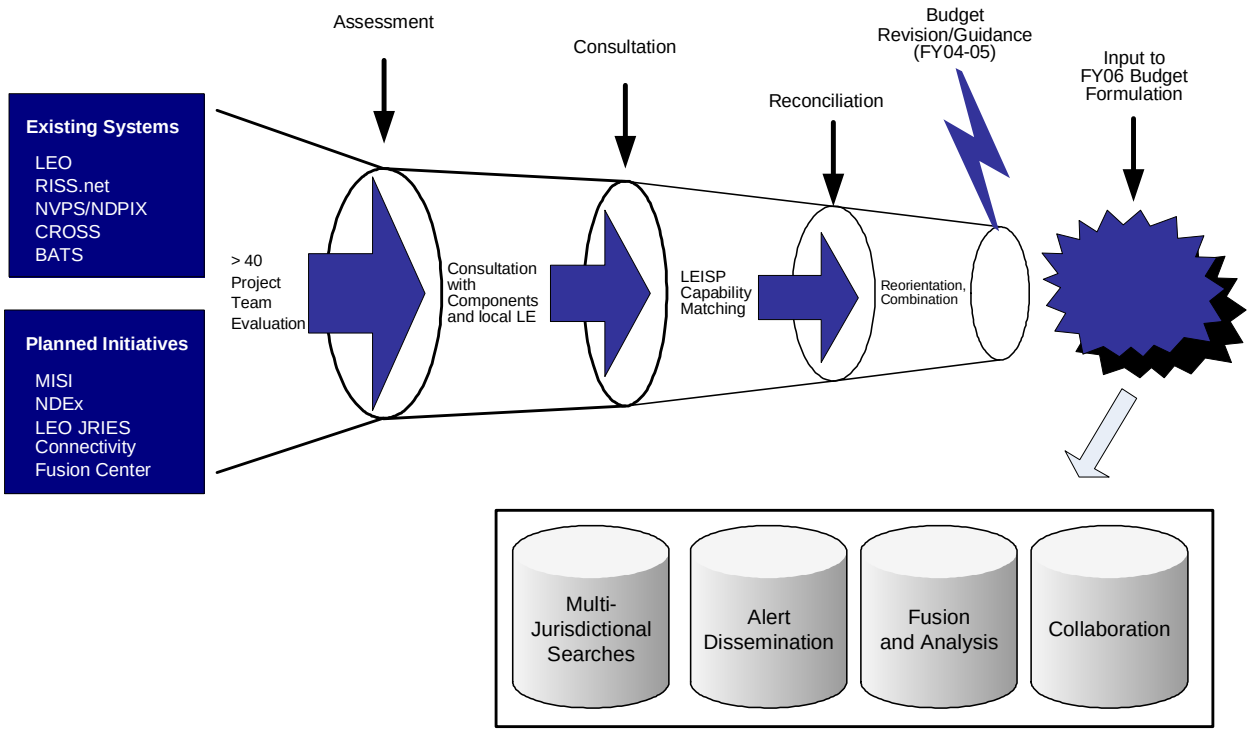
7.2.1.2 Common De-Confliction Procedures

The Department will establish common procedures and protocols to coordinate and de-conflict investigative activities across all DOJ law enforcement components and work cooperatively with its partners to extend these procedures to the community. Common de-confliction procedures will ensure maximum cross-jurisdictional cooperation and maximization of resources.

7.2.2. Reconcile and Coordinate Existing and Planned Information Sharing Initiatives and Data Sources

DOJ is currently managing more than 40 existing and planned information sharing systems and internal systems that will provide shareable information. In executing the OneDOJ strategy, the Department has assessed these systems and mapped them to the functional requirements previously detailed. The next step is to develop plans for integration and/or interconnectivity; one of the most significant challenges lies in the fact that most of the data sources were not built to share information. The assessment will be divided into two distinct and separate paths. In one path, the DOJ Chief Technology Officer (CTO) will assess them from a technology and technical architecture perspective. In the other, JICC and the responsible component, in consultation with OCIO and the LEISP Steering Committee, will assess the final business process and law enforcement needs perspective.

Figure 7-3: Existing/Planned Systems Rationalization Process



Upon completion of the assessments, the Department will factor the results into component budget decisions. The goal is to eliminate and/or combine duplicative and overlapping services. At the completion of the process, the Department will place long-term focus on:

- one alert system;
- one pointer system;
- one counter-surveillance reporting system;
- one integrated SBU/LEA email system;
- one consolidated watch list;
- one model for a intelligence/analytical fusion center; and
- one point of connection (or interface specification) for partner access to sharable law enforcement information and services

7.2.3. Deploy Core Capabilities

The Department intends to deploy core capabilities to facilitate access to its law enforcement information, first internally and then with partners following a consultative process.

The Department and its partners recognize that many of these needs and services are long overdue and that existing systems are inadequate. Equally important to all partners are core capabilities that can be made available as soon as practicable, as well as new and more sophisticated services that can be deployed over time.

The first iterations of this core capability will seek to leverage existing initiatives and services as well as to further exploit those national and regional initiatives that can most quickly provide core capabilities to LEISP partners.

7.3. Track 2: Enable Local Law Enforcement Access to DOJ Information

Implementing the LEISP strategy is a long-term effort, but there is also a need for immediate action. As a first step in Track II of the LEISP Implementation Plan, DOJ will start sharing information within the context of existing sharing initiatives between state, local, and tribal law enforcement partners.

7.3.1. Start Information Sharing Now

In order to meet critical information sharing needs as soon as possible and to further demonstrate the Department's leadership toward the national program, DOJ will execute three immediate steps to start information sharing:

7.3.1.1. Establish immediate connection between DOJ and DHS systems.

In consultation with DHS, the Department will connect DOJ's Law Enforcement Online (LEO) and Regional Information Sharing System (RISS) systems with DHS's Joint Regional Information Exchange System (JRIES)/Homeland Security Information Network (HSIN) system.

7.3.1.2. Identify additional DOJ systems that can be made available to the law enforcement community through LEO/RISS.net.

The OCIO will consult with DOJ components to prioritize existing data sources that can be made available for law enforcement communitywide sharing in the near term via the existing LEO/RISS.net platform.

7.3.1.3. Leverage existing or planned investments to support LEISP.

In supporting the LEISP initiative, the Department of Justice (DOJ) intends to leverage as many of its currently existing or planned information sharing investments as possible. As a first step to advance the LEISP architecture, the DOJ has identified two investments that will provide capabilities that map well to the first iteration of LEISP's core functionality. Deployment of these DOJ investments will facilitate increased timely access to DOJ's law enforcement information. The identified investments include the Regional Data Exchange (R-DEx) and the National Data Exchange (N-DEx). Each investment will be the catalyst to fulfill a particular portion of the overall LEISP architecture. R-DEx and N-DEx will provide baseline functionality for full-text search and structured search respectively.

7.3.1.3.1. R-DEx

R-DEx will provide LEISP with full-text search capabilities. Currently, regional intelligence centers (RICs) provide tailored information sharing solutions, based on regional consensus. RICs may provide a wide and varying set of capabilities; this may include capabilities such as phrase-

based and concept-based searching of unstructured documents, such as investigative files. R-DEx will provide an interface to RICs to enable searching of unstructured documents and for retrieving matching documents. The first RIC to interface with R-DEx will be the Seattle, Washington, regional law enforcement information sharing system called Northwest LInX (Law Enforcement Information Exchange). R-DEx will be a data repository for full-text shareable SBU DOJ law enforcement data and will serve two main functions: providing RICs with access to DOJ's data and providing DOJ users with access to regional information. R-DEx's data will be regionally partitioned, enabling a RIC's users to perform full-text searches over DOJ unstructured documents for the region, in addition to the state and local documents accessed internally.

7.3.1.3.2. N-DEx

N-DEx will provide the first implementation of structured search and index for LEISP. A wide variety of data (e.g., structured, full-text, multimedia) will be available through N-DEx, although searching, matching, and linking will only be possible on well-defined entities (e.g., people, vehicles, locations, weapons, phone numbers), not on arbitrary text (full-text data). All law enforcement agencies will be encouraged to share as much data as possible through N-DEx. At first the focus will be on structured incident data, but eventually it will expand to other structured data as well (extracted entity data from full-text documents). However, N-DEx will maintain a link to the document and will be able to retrieve the document for presentation to the user. Initially, the focus will be on large agencies and aggregated data sources such as RICs, but eventually it will expand to any law enforcement agency. LEISP intends to eventually include all shareable SBU DOJ criminal incident data in N-DEx.

7.3.1.4. Participate in regional sharing initiatives.

The Department has identified a number of ongoing regional information sharing initiatives in which DOJ may wish to participate. The Department will establish appropriate standards for joining these initiatives, including standards for data ownership, de-confliction, auditing, security, privacy protection, technology interfaces, and other MOU issues.

7.3.2. Collaborate To Develop One-Way Connection to DOJ

Advancing the value of OneDOJ to the national community will require extensive collaboration to leverage the experience gained in efforts to build the distribution channels necessary to allow DOJ's partners to connect. Collaborative work steps necessary to achieve one-way connection to LEISP strategy capabilities will require:

- technology architecture requirements for partners to achieve automated connectivity to LEISP capabilities;
- relevant partner policies; and
- funding requirements.

7.4. Track 3: Enable Multi-Directional Information Sharing

Multi-directional information sharing between DOJ and its federal, state, local, and tribal law enforcement partners is the end-state vision of the LEISP strategy. This vision will require

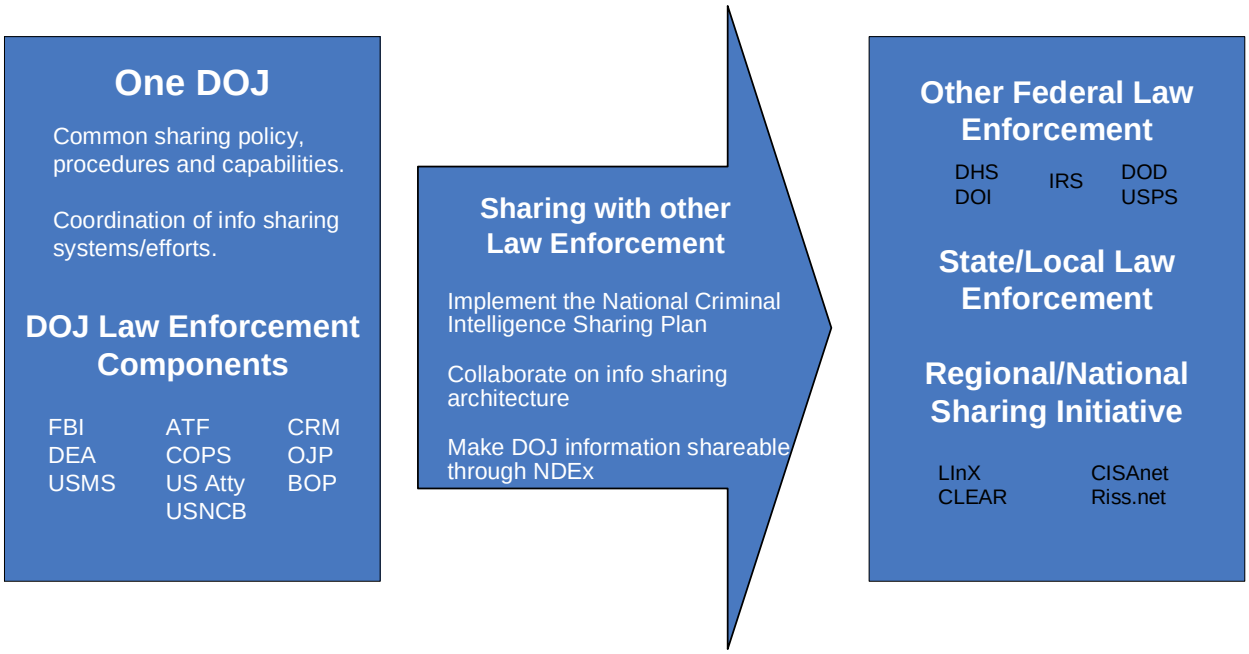
significant alignment of partner systems with DOJ systems, an alignment that DOJ cannot dictate. The Department realizes that the vision will require the creation of an extensive collaboration process between DOJ and its partners. The work steps in this collaborative process will include:

- technology architecture that will enable the ability of DOJ's federal, state, local, and tribal law enforcement partners to publish their information for availability in the sharing environment
- relevant partner policies that apply to multi-directional information sharing
- funding requirements for multi-directional information sharing
- privacy requirements for multi-directional information sharing

7.5. Implementation Collaboration Management

This section of the implementation plan describes the framework DOJ will deploy to ensure that the LEISP strategy is executed with maximum outreach and collaboration, both within DOJ and between DOJ and its federal, state, local, and tribal law enforcement partners.

Figure 7-4: LEISP Strategy-Law Enforcement Partner Collaboration Framework



7.5.1. Technology Architecture Collaboration

The Department, in consultation with its components, engages technical working groups with Global and CJIS APB to address critical issues that will emerge during Track II activities to enable local law enforcement access to DOJ information and Track III activities to enable multi-

directional information sharing. These consultations will address the topical objectives that will need to be resolved in regard to standards, interoperability, and architecture. Examples include:

- developing an inter-networking strategy to reflect the reality that the vast majority of local law enforcement agencies do not have the existing infrastructure necessary to support Internet-based activities for on-demand data or record retrieval
- matching the LEISP architecture to technical standards that are incorporated into state architectures
- identifying/agreeing to data standards that leverage the successes realized through existing regional and local cooperative information sharing efforts
- designing adaptors when necessary to allow local law enforcement to contribute data to the information sharing environment. This work must reflect the challenge of building adaptors to many diverse records management systems, case management systems and other source data systems
- developing a strategy to distribute the LEISP architecture across state's law enforcement agencies and thereby giving local law enforcement the ability to leverage existing statewide communications infrastructure and more effectively target upgrades where needed to support LEISP
- coordinating the developing LEISP standards and architectural concepts with those of the "Plan for the Interoperable Terrorism Information Sharing Environment" in response to Executive Order 13356

7.5.2. Architecture Principles

In the course of collaboration efforts to date, a series of architectural principles and objectives will be compiled into the OneDOJ framework. Many of these current and emerging principles have come from internal DOJ partners and other federal systems as well as from the state and local law enforcement representatives to the LEISP to date. Examples include:

- Re-use of Existing Systems and Infrastructure. Many projects and systems exist today that can be leveraged as a part of the LEISP solution. Architecture decisions should not ignore or obviate these existing investments, but instead provide a migration path for all technologies to connect and consume common services.
- Promote Open Standards and Vendor-Neutral Solutions. Through the promulgation of industry and community standards for the proposed architecture, more partners and solutions can be simultaneously managed into the future environment. Providing for vendor neutrality at once allows competitive solutions for thousands of partner implementation and requirements, and precludes architecture components from obviating existing platforms and technologies already available among LEISP partners.
- Distributed Data. Shared data should reside with the law enforcement agency that owns it. This enables law enforcement agencies to maintain full control over their data and obviates the need for a separate, expensive, and centralized data warehouse. Caching can be provided to help some law enforcement agencies meet access performance requirements.
- Security and Privacy. Architectural design is predicated on first developing an interoperable set of policies and agreements for the operation of an LEISP system, and management of Security and Privacy will remain priorities in the development of LEISP

integration capabilities. The system ultimately needs to be policy-driven by a framework of partners' requirements.

- Integration Options. Allowing a less stringent integration option provides a phased implementation path and enables more systems to join LEISP sooner. In addition, such a flexible integration option encompasses systems that could not meet the more standardized option. A standardized integration option, on the other hand, allows for the development of more powerful, coordinated functionality. The LEISP architectural approach needs to be mindful of the disparity of technologies and resources across its partners, where those resources and existing systems do not solely drive solutions that cannot be managed or afforded by the majority of the partners. Flexibility in the methods and means of integration will be critical to the wide and long-term success of the LEISP architecture.
- Reusable Adapter Technology. Providing pre-built, reusable components for building adapters to legacy systems will significantly reduce the cost and risk of integrating legacy systems into LEISP, as well as ensuring compliant interface implementations.
- Rigorous Auditing. Sharing sensitive data with other law enforcement agencies through LEISP requires trust that Memoranda of Understanding are being properly implemented, regardless of who owns the hardware implementing them. Trust is achieved and maintained through verification – in the case of LEISP, through rigorous auditing. Law enforcement agencies must be able to see who is accessing their data, how often, when, and why.

The architecture sought will embody these principles. Universally, functional requirements suggest that the following services be developed and managed for the LEISP partners:

- Data sources can implement a simple standard interface to share their data items with the system, and are controlled and administered by individual law enforcement agencies.
- Data sources support all the coordinated functionality of the LEISP system, including immediate searching through the LEISP and notification of new data items through subscription. If desired and authorized, complete data items can be retrieved from their original sources.
- Fulfillment centers provide a more flexible integration option for a wider array of systems, but do not necessarily provide the same level of LEISP functionality.
- Bulk retrieval and "fusion" provide a special mechanism to support analytic processing, without requiring the mandatory warehousing of LEISP data.
- All significant LEISP transactions are logged, and all logs are data sources, so that the full power of searching and subscription can be used for auditing.

7.5.3. Policy Collaboration

Previous chapters of this strategy document detail information sharing policies for DOJ and policy areas that will need to be developed cooperatively with partners. The Department will work with Global and the CJIS APB on reaching consensus on policies for partner law enforcement agencies.

7.5.4. MOU Creation and Execution Collaboration

The rules to which DOJ and information sharing partners will commit will be formalized through the mutual development of Memoranda of Understanding (MOU). In consultation with Global and CJIS APB, the Department will develop templates for MOUs in order to standardize format and content requirements. Next, the Department will work with Global and CJIS APB to provide advice and counsel on customizing and executing the MOUs as appropriate. Where the Department participates in existing regional information sharing initiatives, MOUs will be executed through the regional information sharing organization.

7.5.5. Privacy Collaboration

Privacy considerations are a critical component of the LEISP strategy. Protection of privacy is paramount to guiding principles. The Department is committed to putting the privacy considerations foremost in implementation plans. The Department will develop all required Privacy Impact Assessments and Systems of Records Notices. The Department's Chief Privacy Officer will advise LEISP on the protection of individual privacy throughout implementation of the LEISP strategy, and will develop a privacy policy that outlines all legal and policy considerations applicable to LEISP.

7.6. Implementation Coordination

The following activities will focus on executing a range of activities to ensure overall coordination of the LEISP strategy:

7.6.1. Communications Planning

Throughout the implementation of the LEISP strategy, there will be a strong requirement for communication between and among partner organizations. A comprehensive communications plan is being developed that focuses on ensuring that relevant stakeholder groups have been informed of the processes and status of LEISP implementation and have been given sufficient opportunity to respond, ask questions, and get their questions answered. Partners will have an active role in helping to craft the appropriate communication messages and materials for their constituencies, and in delivering those communications.

7.6.2. Coordination of LEISP Through Program Staff

Program staff will be assigned, as appropriate, to ensure that the LEISP strategy can be fluidly executed across the DOJ enterprise and translated quickly into action. This staff will primarily serve in a coordinating role, supporting strategic planning, business processes change planning, and project management. Specific functions that will be undertaken by the LEISP staff include:

- coordination of DOJ-wide and interagency policy issues through the JICC and the LEISP Steering Committee
- coordination and strategic planning assistance to DOJ components as they undertake individual implementation projects, including process change initiatives and ensuring that project implementations are consistent with the strategy
- coordinating and integrating DHS and other federal agency information sharing initiatives with the LEISP strategy

- serving as the DOJ Department-level liaison with state, local, and tribal law enforcement agencies throughout their participation in LEISP
- providing direct LEISP-related staff support to the Office of the Deputy Attorney General (ODAG) and the JICC, including administrative support for MOU processes, privacy impact assessment, budgetary development and tracking, implementation plan development, and progress tracking
- assisting in the development and management of Department-level internal and external communications and outreach activities

7.7. Program Management

LEISP program management activities will focus on organizing and managing resources to complete individual projects according to their individual program lifecycles. LEISP project-specific management will be the responsibility of DOJ components and individual federal, state, local, and tribal law enforcement partners, with the exception of Department-wide LEISP initiatives managed by the OCIO. Important program management activities include:

- identifying business and technical requirements needed to implement LEISP core services and managing their implementation
- identifying business and technical requirements needed to implement other LEISP services and coordinating their implementation through DOJ components
- identifying business process requirements and capabilities for partners to comply with MOU mandates, (e.g. auditing, quality assurance, privacy) and identifying strategies and approaches for training, education and capability development
- developing plans and sequencing approaches for agency integration
- coordinating DOJ cross-component projects, including plans for large system interoperability with LEISP

Project management activities that will be the responsibility of individual components will include:

- managing the individual component projects that implement the LEISP strategy, except projects assigned to the OCIO
- managing the scope and development lifecycle for individual agency projects to coordinate with LEISP timeframes
- defining the specific procedures for implementing LEISP requirements, such as data sharing, security and privacy policies
- implementing individual agency connectivity to LEISP, including specific design, programming, testing, and conversion requirements within Department-wide standards and guidelines

8. Next Steps: Building Partnerships

As outlined in section 7, the three key tracks of the LEISP will run concurrently. Even as significant steps have already been made in Track I (Creating OneDOJ), the fundamental step is to get DOJ's information sharing house in order. Updates to the LEISP strategy will be published as policy and technology updates become available. Recognizing the developing nature of information sharing strategies, the Department invites all potential law enforcement partners to provide comments and input for the ongoing development process of the LEISP.

Anticipated process steps are as follows:

- Complete strategy collaboration process
- Review requirements and principles and develop specific policy guidelines
- Review principles and develop LEISP Track II and III architecture components
- Pilot proof-of-concept Track II information sharing project(s)
- Pilot proof-of-concept Track III information sharing project(s)

In each step, all tracks of development are in progress. As the Department works toward a multi-year goal of completing the OneDOJ (Track I) framework, many potential projects (or proof-of-concept opportunities) that fit the Track II and Track III requirements are anticipated, with existing and emerging local and regional information sharing efforts having been identified as likely candidates for early proof-of-concept models. It should be clearly understood that the requirements and outputs of Tracks II and III component deliverables are not predicated on the completion of preceding phases.

The Department, moreover, seeks to invite and collaborate with law enforcement partners and projects, and anticipates growth in these areas over time. The Department will continue to reach out through relationships with it federal, state, local, and tribal law enforcement partners, with national organizations, and with others who support law enforcement in order to garner participation, input, and partnerships within the program.

As a collaborative process, the Department cannot control or predict timelines for deliverables of Tracks II or III, but seeks to enter into partnership projects as soon as practicable following completion of the organizational requirements tracks.

The Department, again, expresses its appreciation for the time and consideration of all agencies and staff who have invested time and effort in the creation of this strategy, as well as the review and feedback of this draft document. The Department would also like to express gratitude to the many focus group participants who helped shape our current understanding of the needs and requirements for a national law enforcement information sharing program. The Department looks forward to continuing a constructive and growing collaborative partnership with all members of the law enforcement community as the nation moves forward with this important initiative to improve law enforcement information sharing.