DEPARTMENT OF HOMELAND SECURITY

INTERACTION WITH STATE AND LOCAL FUSION CENTERS

CONCEPT OF OPERATIONS

DECEMBER 2008

1.0 Executive Summary

The purpose of this State and Local Fusion Center Concept of Operations (CONOPS) is to establish a framework for a comprehensive, coordinated and consistent approach for outreach by the Department of Homeland Security (DHS) to State and Local Fusion Centers (SLFCs). This CONOPS outlines DHS processes relating to SLFC support including intelligence and operational information flows and interactions, deployment of officers, component integration, and identification of SLFC requirements, technical assistance and training. DHS will also ensure outreach, communication, and integration with other multidisciplinary partners (i.e., fire service, public health, and emergency management), to further ensure and facilitate information sharing between SLFCs and these disciplines. This CONOPS will be periodically reviewed and modified as additional processes are implemented and refinements identified.

The CONOPS provides transparency into DHS support to SLFCs. The CONOPS also:

- Furthers the goals of the Director of National Intelligence (DNI) and the Program Manager Information Sharing Environment (PM-ISE) to develop and support a national information sharing environment and network of fusion centers.
- Underscores the role of the Under Secretary for Intelligence and Analysis as the Executive Agent for DHS SLFC Program and DHS's representative to various Federal Senior-level advisory groups providing guidance and support to fusion centers.
- Defines the roles and responsibilities of the State and Local Program Management Office (SLPO) to execute the DHS SLFC Implementation Plan and to lead DHS outreach to SLFCs which includes, but is not limited to, the assignment of DHS intelligence analysts and officers and the provision of tools to the fusion centers nationwide. The SLPO serves in the central coordination role for DHS interaction with SLFCs.
- Institutionalizes the Single Point of Service (SPS), a coordinated Office of Intelligence and Analysis/Office of Operations Coordination and Planning business process, developed to ensure all SLFC inquires are responded to expeditiously by the appropriate elements within DHS and there is accountability for this transactional activity.

2.0 Introduction

State and Local Fusion Centers (SLFCs) are being created by the States and Major Urban Areas as a way to address the unique information needs of State, local, tribal, and territorial authorities, along with their stakeholders, including the private sector. This information sharing challenge was recognized by the 9/11 Commission. A fusion center is defined as a "collaborative effort of two or more Federal, State, local, or tribal government agencies that combines resources, expertise, and information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal and terrorist activity."[1] Currently, many states have at least one fusion center – several states have multiple centers, an increasing number of cities and counties also have fusion centers, and more are anticipated. The fusion centers are established, managed, and controlled by State and local entities and are subject to political and legal constraints within their respective jurisdictions. Each fusion center is developed to meet the unique needs of its area of responsibility. Today, SLFCs serve a pivotal role within their States for the sharing and fusing of homeland security-related information and intelligence.

Recognizing the role of fusion centers in protecting the homeland, the Department of Homeland Security (DHS) has been actively working to develop strong partnerships with SLFCs. DHS is building these partnerships to enhance its missions and to support the diversity of the counter-terrorism, all-crimes, and all-hazards missions of the SLFCs. These relationships expand upon DHS components' established cooperation and functional coordination with State and local governments, within their individual mission areas.

Guided by the *Department of Homeland Security Support Implementation Plan for State and Local Fusion Centers*, and under the leadership of the State and Local Program Office (SLPO), intelligence professionals from the DHS Office of Intelligence and Analysis (I&A) have been assigned to work with State and local authorities in SLFCs across the country. Personnel from DHS agencies and components are also working with SLFCs in support of their respective missions. DHS has also assumed a key role in providing training, grants, and other operational support to the SLFCs. As a result, many different DHS components are involved in developing partnerships and helping facilitate the two-way flow of timely and accurate information authorized by law on all types of hazards.[2]

---

[1] *Implementing Recommendations of the 9/11 Commission Act of 2007.*

[2] State and Local Fusion Center Web page, http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm

On August 3, 2007, President George W. Bush signed into law the *Implementing Recommendations of the 9/11 Commission Act of 2007* (hereafter referred to as the 9/11 Commission Act) [3]. In part, the 9/11 Commission Act directs DHS, in consultation with the program manager of the information sharing environment[4] and the Attorney General, to establish a State, Local, and Regional Fusion Center Initiative. DHS's SLFC Program addresses many of these requirements[5]. DHS will enhance the existing SLFC Program to address all of the elements of the 9/11 Commission Act. The 9/11 Commission Act also specifies that a Concept of Operations (CONOPS) be developed for the program and submitted to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

2.1 Scope

This CONOPS was originally initiated in response to a request from the DHS Information Sharing Governance Board (ISGB) in April 2007. Because the 9/11 Commission Act also requires a CONOPS to address the SLFC Initiative, the project was subsequently expanded to include the requirements of the 9/11 Commission Act. Specifically, the CONOPS:

- Provides a clear articulation of the purposes, goals, and objectives of the SLFC Program;
- Defines the mission-specific support to the fusion centers provided by DHS writ large;
- Identifies principal stakeholders in the SLFC Program at the Federal level;
- Acknowledges the Baseline Capabilities for State and Major Urban Area Fusion Centers as the framework from which measures of effectiveness for fusion centers can be developed;
- Institutionalizes the Single Point of Service (SPS) Concept to ensure SLFC requests for support are handled expeditiously; and
- Includes both Privacy and Civil Liberties Impact Assessments.

This CONOPS builds upon the *Department of Homeland Security Support Implementation Plan for State and Local Fusion Centers* and further defines the coordination and oversight role of the Under Secretary for Intelligence and Analysis as the Executive Agent of the DHS SLFC program. It advances DHS's role in fulfillment of Initiative 5c of the DNI's *United States Intelligence Community (IC) 100 Day Plan - Integration and Collaboration*, to support Program Manager for the Information Sharing Environment (PM-ISE), Federal Bureau of Investigation (FBI), and DHS efforts to share with State, local, tribal, and private sector entities.

---

[3] Public Law No. 110-53, 121 Stat. 266 (Aug. 3, 2007) (amending, in relevant part, the Homeland Security Act of 2002, Public Law No. 107-296).

[4] *The Intelligence Reform and Terrorism Prevention Act* defined the "information sharing environment" as "an approach that facilitates the sharing of terrorism information."

[5] Hereafter, the CONOPS will refer to the SLFC Program and Initiative interchangeably.

It also advances Initiative 2.C ("Provide Collaborative Information Technology to Non-IC Partners") of the subsequent *500 Day Plan* as well as the *PM-ISE Implementation Plan*, which called for a national network of State and Major Urban Area fusion centers.

This CONOPS also supports the *National Strategy for Information Sharing* released in October 2007. The *Strategy* focused on unifying the nation's information sharing efforts and called for the identification within each state of a primary fusion center for counter-terrorism information sharing. The CONOPS is intended to complement the *Coordinated Department of Homeland Security and Federal Bureau of Investigation Support Plan for Fusion Centers*, currently under development. Lastly, this CONOPS advances the PM-ISE's *Implementation Plan* goal of ensuring that tailored actionable information and situational awareness is enhanced at all levels of government. [6]

The CONOPS establishes a framework for a comprehensive, coordinated and consistent information sharing approach to enable DHS to interact with SLFCs more effectively and efficiently. It creates a structure from which standard operating procedures (SOPs) can be developed. By providing greater visibility across the Department regarding DHS interactions with SLFCs, this CONOPS improves internal DHS business processes for intelligence and operations information flows and interactions, including activities such as training, operations, technical assistance and infrastructure protection support. This CONOPS will be continually reviewed and modified as processes are implemented and refinements identified.

2.2 Guiding Principles

The following guiding principles were established to ensure the CONOPS provides an effective integrating tool for the Department and its individual components in fulfilling their respective missions with the SLFCs:

- I&A—specifically the Chief Intelligence Officer (CINT) - is the Executive Agent for Departmental interaction with SLFCs, and will maintain visibility and a coordinating role with respect to SLFCs;
- Adhere to the unified DHS concept known as "One DHS"[7] and the *DHS Information Sharing Strategy*;

---

[6] "For SLT governments: It must create a recognizable Federal focus for federally coordinated terrorism information, one that generates more tailored, actionable information and improves situation awareness at all levels and supports the development of a true national analytic capacity." *(Information Sharing Environment Implementation Plan)*

[7] In February of 2007, the DHS Secretary issued a memorandum referred to as the "One DHS" memorandum that sets forth the concept of unification across all DHS Component agencies. It established as official policy a procedure that enables information sharing with respect to one DHS Component agency, and applies equally to other agencies within DHS.

- Synchronize DHS support with the missions of the SLFCs to ensure the appropriate sharing of information and assignment of personnel;
- Do not inhibit or restrict existing, effective relationships with DHS representatives, but serve to further enhance these relationships by providing greater clarification of roles and responsibilities;
- Leverage the best practices for information sharing, and revise existing processes when necessary and advisable;
- Ensure information shared or distributed fulfills Constitutional, statutory, regulatory, and other legal and policy requirements, as appropriate, including applicable Privacy and Civil Liberties standards. These include, but are not limited to, the Fourth, Fifth, and Fourteenth Amendments to the Constitution; the Privacy Act of 1974; 28 CFR. Pt. 23; Executive Order (EO) 12333; directives issued by the President, DHS, the Department of Justice, and the IC; and other guidance provided by the PM-ISE; the National Strategy for Information Sharing (NSIS); and
- Periodically review to ensure accuracy and to incorporate process improvements.

3.0 Purpose, Goals, & Objectives

This section describes the purpose, goals, and objectives of the DHS SLFC Program to provide context for the processes outlined in the remainder of the CONOPS.

The purpose of the SLFC Program is to establish partnerships with State, local and regional fusion centers that facilitate the lawful sharing of homeland security information and intelligence. The SLPO, as the day-to-day manager of the SLFC Program, has articulated three goals:

- Goal 1: Establish DHS Presence in SLFCs: Ensure all SLFCs have a robust DHS presence by deploying personnel and information systems, as appropriate.

- Goal 2: Enable the National Fusion Center Network: Develop and implement an intelligence and information capability that further professionalizes the SLFCs and strengthens their ability to add value to the national knowledge base, while preserving individual privacy and civil liberties.

- Goal 3: Operate and Sustain Investment and Activities: Ensure DHS equities in SLFCs support information sharing and intelligence cycle activities throughout the national fusion center network. Provide robust support to DHS staff assigned to SLFCs and update tools and information systems as necessary.

Consistent with the 9/11 Commission Act and to achieve its stated purpose, the Secretary of Homeland Security, through the SLFC Program, with principal officials from State and local authorities, have established the following objectives:[8]

- Provide operational and intelligence advice and assistance to State, local, and regional fusion centers;
- Support efforts to include State, local, and regional fusion centers into efforts to establish an information sharing environment;
- Ensure the conduct of well-coordinated DHS tabletop and live training exercises to regularly assess the capability of individual and regional networks of State and Major Urban Area Fusion Centers;
- Integrate the efforts of individual and regional networks with the efforts of the Department;
- Coordinate with other relevant Federal entities engaged in homeland security-related activities;
- Provide analytic and reporting advice and assistance to State, local, and regional fusion centers;
- Review information within the scope of the information sharing environment, including homeland security information, terrorism information, and weapons of mass destruction information, that is gathered by State, local, and regional fusion centers, and incorporate such information, as appropriate, into the Department's own such information;
- Provide management assistance to State, local, and regional fusion centers;
- Provide a point of contact to ensure the dissemination of information within the scope of the information sharing environment, including homeland security, terrorism, and weapons of mass destruction information;
- Facilitate close communication and coordination between State, local, and regional fusion centers and the Department;
- Provide State, local, and regional fusion centers with expertise on Department resources and operations;
- Provide training and technical assistance to State, local, and regional fusion centers; and
- Carry out such other duties the Secretary deems are appropriate.

[8] From the *9/11 Commission Act of 2007, § 511.*

3.1 DHS/SLFC Interaction Desired End State

The successful implementation of this CONOPS will create an environment in which DHS resources are aligned to achieve the stated purpose, goals, and objectives: enable SLFC partnerships, enhance the lawful sharing of information, and coordinate interactions with SLFCs consistent with the Department's statutory mission as defined by the Homeland Security Act of 2002, as amended. This environment comprises five essential elements: Communication, Collaboration, Understanding, Coordination, and Management Support.

Communication

DHS will ensure that communication with SLFCs is efficient and effective. The Department has created the Single Point of Service (SPS) for DHS information and intelligence support to State and local fusion centers to ensure that all inquires are responded to expeditiously by the appropriate elements within DHS. The SPS process is discussed in detail later in the document. The SPS will not preclude the SLFCs from interacting with DHS components directly. The SPS will be responsible for identifying the appropriate DHS resources to address requests, providing transparency across DHS entities, and tracking requests through to completion. DHS will continue to enhance its relationships with the SLFCs, including by providing mechanisms to improve visibility to the appropriate stakeholders of DHS activities, such as analysts' conferences and regular DHS representative visits to the fusion centers. The Department will continue to develop other communications tools, including the Homeland Secure Data Network (HSDN), the Homeland Security Information Network (HSIN) and the HSIN-Intelligence portal —to improve communications with fusion centers. DHS will develop, within the framework of this CONOPS, Standing Operating Procedures (SOPs) to determine the specific organizations within DHS associated with specific types of SLFC interactions. These SOPs will address coordination of interactions across the Department in greater detail.

Collaboration

To enhance the partnership with SLFCs and deepen connections between DHS and SLFC analysts, DHS will expand existing collaborative analysis, assessment, and planning capabilities. DHS will continue to develop mechanisms to more effectively identify opportunities to collaborate to include the Fire Service, Public Health, and Emergency Management. DHS and SLFCs will expand the development of joint products and explore tools to improve the collaborative environment. The Department will also continue to support and develop collaborative bodies like the Homeland Security State and Local Intelligence Community of Interest (HS-SLIC). Operational components, in concert with the SLPO and other components, will conduct strategic planning, including resource projections, necessary to support field interactions with SLFCs.

Understanding
As partnerships expand and are strengthened, DHS and the SLFCs will enhance their understanding of each other's capabilities and needs. DHS will enhance support to SLFCs on three critical dimensions of information support:

- Response to the SLFCs' requests for information;
- SLFC Priority Information Needs (PINS) that align with I&A analytic production to SLFC needs; and
- Training and technical assistance tailored to the needs of the SLFC analytic cadre.

The Department will expand its active engagement of SLFCs to understand their needs. SLFCs will better understand how information can be combined at the Federal level, and what types of DHS support are available and appropriate to meet their needs. Further, DHS will continue to work with the fusion centers to maintain an open dialogue about needs and capabilities and will educate the fusion centers on DHS headquarters and component capabilities. DHS will also provide SLFCs feedback on information received, and identify the types of information most useful for integration into DHS products.

Coordination
DHS will continue to develop processes and tools to increase the transparency of activities and information exchanged with the fusion centers. All DHS components will be able to quickly view the recent and planned activities, such as conferences or site visits. The SPS will continue to facilitate coordination among the DHS components and ensure requests are responded to in a timely manner. The DHS Homeland Security Intelligence Council's Integrated Intelligence Board (HIIB), a body composed of the heads of intelligence functions from all DHS components and chaired by the Chief Intelligence Officer, will ensure mechanisms are in place to coordinate across DHS on analytic collaboration with SLFCs. Similar mechanisms will be implemented to provide visibility into products distributed to or available to the fusion centers, as well as training opportunities or assistance to increase awareness of what information and resources fusion centers have access to.

Management Support
In an effort to establish a baseline level of capability in all fusion centers through the implementation of the *Global Fusion Center Guidelines* and the *Office of the Director of National Intelligence – Information Sharing Environment Implementation Plan*, DHS will continue to provide an integrated suite of support programs. DHS may revise the Homeland Security Grant Program Guidance as needed to enable the full implementation of the fusion process. In addition, the joint DHS/Department of Justice (DOJ) Fusion Process Technical Assistance Program will continue to support the establishment of baseline capabilities through the following activities:

- Fusion Process Technical Assistance Services;
- Fusion Center Exchange Program;
- Fusion Center Fellowship Program;
- Online Fusion Process Resource Center; and
- Other Specialized Fusion Process Support Services.

4.0 Stakeholders

The SLFC Program furthers partnerships with the fusion centers to facilitate lawful mission-oriented information sharing and operations coordination within and between the centers, as well as with other DHS stakeholders and other Federal agencies. As such, stakeholders for the SLFC Program include: the State, local, and tribal entities, DHS components and other Federal agencies, the private sector, and the American public.

DHS components, including those with primarily law enforcement missions, both in the field and at headquarters, are important stakeholders. State and local information shared by SLFCs and combined with information acquired elsewhere by DHS and its Federal partners allows DHS to develop a more complete picture of potential threats and emerging incidents.

Federal agencies, external to DHS, are also stakeholders in the SLFC Program. For example, DHS partnered with DOJ, PM ISE, and the Global Justice Information Sharing Initiative to define fusion center baseline capabilities. The FBI and other agencies with law enforcement responsibilities are also stakeholders in information sharing and coordination with the SLFCs.

Finally, other Federal agency stakeholders include those designated Sector Specific Agencies by Homeland Security Presidential Directive (HSPD) 7 for coordinating infrastructure analysis and protection.

The definitive stakeholder and benefactor is the American public. Citizens are key participants in providing information regarding suspicious activities or concerns with the proper authorities. Information provided by the public is crucial in developing timely and actionable intelligence, as well as in responding to events or incidents. The proactive and continual sharing of information is also the best mechanism to prevent and respond to all threats.

5.0 Functional Roles and Responsibilities

DHS has as a mission to be the primary Federal source of accurate, actionable, and timely homeland security-related information for its State, local, tribal, and private sector partners. The 9/11 Commission Act outlines a broad set of responsibilities for the Department in relation to SLFCs, ranging from providing

operational and intelligence advice and assistance, to conducting tabletop and live training exercises, to providing management assistance. Additionally, in December 2005, the President instructed the Secretary of DHS and the U.S. Attorney General to create a national integrated network of State and Major Urban Area fusion centers. DHS carries out these missions through the work of its component organizations and through its participation in interagency groups.

DHS participates in three key interagency groups that support the development of an information sharing framework between and among SLFCs. Through the Interagency Threat Assessment and Coordination Group (ITACG), the National Fusion Center Coordination Group (NFCCG), and the Global Justice Initiative, DHS leads Federal government outreach to the State and local levels. DHS co-leads two of these groups, the NFCCG and the Global Justice Initiative, in conjunction with the DOJ. In the case of the ITACG, DHS chairs the ITACG Advisory Council created by the 9/11 Commission Act and assigns a senior DHS intelligence official to the NCTC to manage the day-to-day operations of the ITACG.

In June 2006, the Secretary of DHS designated I&A as the Executive Agent for the SLFC Program. As a result, I&A provides the leadership and governance of the Department's multiple relationships with the SLFCs. In this role, I&A is responsible for coordinating these relationships across the Department, and engaging component organizations to collaboratively build strong connections for lawful and appropriate information sharing. I&A divisions provide initial analysis of SLFC information and evaluate and respond to State and Local Support Requests (SLSRs). I&A's analytic divisions serve critical roles in the SLFC relationship as well, supporting information requirements and requests, providing context for information, and developing joint products with the fusion centers.

5.1 DHS SLFC Program Management

DHS established the SLFC Program and SLPO to proactively address DHS support to the fusion centers. The SLPO is assigned by the Under Secretary for Intelligence and Analysis as the day-to-day manager of the program, and is responsible for program execution and operational coordination. The SLPO is responsible for ensuring compliance with Congressional directives and reporting on program process. The SLPO will work with the Privacy Office, the Office for Civil Rights and Civil Liberties (as well as the Privacy and Civil Liberties Oversight Board, once operational), the DHS Office of the Inspector General, and the Office of General Counsel to ensure its compliance with appropriate laws and regulations.

Direct Support to Fusion Centers

Among the SLPO's principal responsibilities is the coordination of DHS support to the SLFCs.

Needs Assessments

The SLPO is responsible for conducting needs and capabilities assessments of the SLFCs in order to prioritize placement of personnel and tools. Once assessments are completed and if the determination is made to deploy DHS personnel to SLFCs, the SLPO is responsible for deploying personnel to the field. This responsibility includes, but is not limited to:

- Designating SLFCs for assignment of personnel;
- Hiring DHS intelligence operations specialists for specific SLFCs;
- Working with DHS offices to identify personnel to be assigned to the centers;
- Training selected personnel;
- Providing leadership and management support to DHS I&A intelligence operations specialists assigned to the SLFCs; and
- Coordinating the development and execution, with the Privacy Office and the Office for Civil Rights and Civil Liberties, of the privacy and civil liberties training program for SLFC staff.

Coordination

The DHS Support Implementation Plan for State and Local Fusion Centers also calls for the creation of integrated DHS teams in SLFCs that include both operational and intelligence personnel.[9] DHS has established a DHS State and Local Integration Working Group (SLIWG), Chaired by the Director of the SLPO, under the leadership of the Deputy Under Secretary for Field Operations (DU/S-FO), and composed of representatives from the Department's components to include US Customs and Border Protection (CBP), US Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), US Coast Guard (USCG), I&A and National Protection and Programs Directorate (NPPD). The mission of the SLIWG is to enable the broadest coordination of all appropriate DHS elements in the establishment of a national network of state and local fusion centers.

Resource and Budgeting

The SLPO is also responsible for budget development and execution; administrative support to assigned personnel; coordination and prioritizing

[9] The 9/11 Commission Act states that the: "Under Secretary for Intelligence and Analysis shall, to the maximum extent practicable, assign officers and intelligence analysts from Components of the Department to participating State, local, and regional fusion centers." Officers and intelligence analysts assigned to participating fusion centers may be assigned in coordination with the respective component heads and in consultation with the principal officials of the participating fusion centers. (9/11 Commission Act, § 511(a)(c)). (9/11 Commission Act, § 511).

delivery of information systems and secure communications to the SLFCs to include the Homeland Secure Data Network (HSDN) and the Homeland Security Intelligence Community; supporting field requests; and coordinating the delivery of training and technical assistance to SLFCs.

Interagency Coordination

Coordinated DHS/FBI Support Plan for Fusion Centers

DHS is working to formally coordinate its support to SLFCs with the FBI. At the request of the Joint Homeland Security Council/National Security Council Information Sharing Policy Coordination Committee (PCC) of the *Coordinated DHS/FBI Support Plan for Fusion Centers* is under development and is intended to provide an overview of how DHS and the FBI provide operational support to fusion centers. The Plan supports and is consistent with the Global Justice Information Sharing Initiative's *Fusion Center Guidelines*, and the *Baseline Capabilities for State and Major Urban Area Fusion Centers*.

DHS/I&A Participation in National Level SLFC Advisory Groups

DHS, through the SLPO, participates in two key interagency groups that support development of an information sharing framework between and among SLFCs. Through the National Fusion Center Coordination Group (NFCCG), and the Global Justice Initiative, DHS facilitates Federal government outreach to the State and local levels.

The Global Justice Initiative is a DOJ-sponsored consortium of Federal, State, local, tribal, and territorial agencies working to promote information sharing. It is the Criminal Intelligence Coordinating Committee, which earlier developed and promulgated the 2006 *Fusion Center Guidelines*.

DHS, ODNI, and DOJ have also assembled a collaborative fusion center technical assistance program. This effort, along with recommendations by the Global Criminal Intelligence Coordinating Council, has been identified as meeting SLFC technical assistance needs.

Conferences

DHS, through the SLPO, jointly develops and sponsors annual DHS/DOJ/ISE/Global National Fusion Center Conferences to strengthen the nationwide network of fusion centers. The annual National Fusion Center Conference is designed to support fusion centers as they continue to build their capabilities, while also encouraging continuing Federal, State, local and tribal dialogue in support of fusion centers. Conference participants come from many disciplines, including law enforcement, homeland security, corrections, public safety, and first responders. The Conference is sponsored through a partnership among I&A, Federal Emergency Management Agency (FEMA) National

Preparedness Directorate (NPD), the Department of Justice's (DOJ) Bureau of Justice Assistance and Global Justice Information Sharing Initiative, the Federal Bureau of Investigation, the ODNI and the PM-ISE.

5.2 Operations Support

The DHS Office of Operations Coordination and Planning (OPS) supports SLFCs on a day-to-day basis by providing domestic situational awareness of all threats and all hazards, whether man-made or natural, either through direct notification or via the Common Operating Picture (COP) on HSIN.

OPS maintains program management responsibility for the National Operations Center (NOC) and for HSIN. The NOC is composed of five components:

- Multi-agency NOC Watch;
- Intelligence Watch and Warning (IWW);
- National Infrastructure Coordination Center (NICC);
- National Response Coordinating Center (NRCC); and
- The Planning Element.

HSIN is used by fusion centers to communicate with DHS and among themselves. Operationally, information support – including the COP – is provided to SLFCs through HSIN.

NOC Fusion Cell

The NOC Fusion Cell is composed of the NOC Fusion Desk, I&A IWW desk, and the Infrastructure Protection (IP) desk managed by the NICC. The Cell reaches out to the multi-agency NOC Watch for information as required. SPS analysts and officers review incoming information and intelligence and provide fusion of data to help inform situational awareness around national security and national preparedness goals in a real-time environment. The NOC Fusion Cell assesses, routes, and tracks information received by DHS from the SLFCs. The NOC Fusion Cell will not restrict SLFCs from interacting directly with DHS components or inhibit existing relationships. The NOC Fusion Cell also receives and logs information and requests from SLFCs. Information received is made transparent to other NOC elements, DHS Headquarters elements, and other DHS components through the HSIN network.

National Infrastructure Coordinating Center

The primary responsibility of the NICC is to coordinate operating status awareness of the nation's Critical Infrastructure/Key Resource (CI/KR) with SLFCs. The NICC provides a process and mechanism for information sharing and coordination with government and industry partners. It is a hybrid organization which is organizationally tied to the Office of Infrastructure Protection (IP) in NPPD, and functionally acts as an element of the NOC. The NICC interacts with fusion centers to coordinate with owners of critical

infrastructure and on issues concerning the assessment, protection and restoration of CI/KR. Such interactions may include representatives located in fusion centers or SLFC personnel with responsibility for CI/KR sectors. The NICC is also a member of the SPS through their representatives assigned to the NOC Infrastructure Protection Desk.

National Response Coordination Center
The NRCC will coordinate with State Emergency Operations Centers (EOCs) and SLFCs in response to all hazards incidents. The NRCC is a multi-agency center responsible for the national response and recovery of all hazard incidents that exceed State capabilities. They may also coordinate with SLFCs depending upon the responsibilities assigned to the EOC by the State government.

NOC Watch
The NOC Watch is a multi-agency NOC component that monitors all threats and all hazards to provide situational awareness to DHS senior leadership, other senior government officials, and homeland security partners via direct notification and/or the COP. The NOC Watch interacts with SLFCs through the SPS and through officers assigned to the NOC from State and local agencies. Relevant information received from SLFCs is integrated into the COP by the NOC Watch. Support to SLFCs also includes responding to inquiries sent to the NOC Fusion Cell or to the various Federal, State and local law enforcement representatives in the NOC.

5.3 Information Sharing, Requirements, and Analytical Support

The success of SLFCs will be greatly facilitated by Federal support of SLFC intelligence functions. Given the growing diversity of the SLFC network, DHS has made significant strides in expanding support to these vital entities. The Department has strengthened DHS intelligence support to SLFCs through the deployment of I&A representatives, the establishment of the HS-SLIC[10] to link SLFC partners and Federal Intelligence Operations Specialists, and the dissemination of an expanding number of intelligence products via HSDN and HSIN-Intelligence.

Single Point of Service
I&A is taking a number of additional steps to create a centralized structure for an SLFC-centered intelligence process that provides the intelligence support SLFCs need to carry out their mission. This initiative is a front-end integrated support

[10] HS-SLIC is a community of interest sponsored by DHS dedicated to collaboration among intelligence analysts at the Federal, State and local levels.

organization providing SLFCs the SPS.[11] It endows I&A with full visibility into and accountability on all SLFC information needs and requirements, and proactively disseminates information to the SLFCs to support State decision-making and analytic collaboration. This support includes managing SLSRs, developing joint analysis products, and distributing intelligence products to SLFCs.

The SPS is composed of representatives from the Collections Requirements (CR) Division, the Reporting and Production (RP) Division, the SLPO, and the NOC Fusion Cell.

I&A will extend the SPS concept for SLSRs to all fusion centers. A SLSR includes requests from State and local law enforcement and members of the traditional IC. For example, a SLSR can include requests for information, intelligence, administrative support, and other assistance or interaction.

SPS staff will participate in the responsibilities of assessing and routing incoming information and requests received from SLFCs. The IWW analyzes information received from a variety of sources including SLFCs to determine if it is of intelligence significance. It routes SLFC and other intelligence information to the relevant I&A division for integration into intelligence products. The IWW integrates information with additional contextual intelligence and distributes daily threat products to the fusion centers.

RP assigns the SLSR to the appropriate I&A analytic divisions for response on behalf of SPS. It also distributes finished intelligence products to the SLFCs. PM receives, develops, disseminates, and posts DHS threat products to SLFCs, and other partners, through a highly-articulated vetting and dissemination process. Its expertise lies in identifying existing DHS and stakeholder needs and mechanisms, explicitly including those of and relating to SLFCs, for the orderly dissemination of products to appropriate parties, congruent with specific threat and countermeasure information and capabilities. This assures that products are effectively disseminated to those who need them, but only if they are duly authorized to receive the information, based on product classification level and recipient need-to-know.

SLSRs that are intelligence related from the SLFCs are managed and responded to by the CR on behalf of the SPS. Requests from SLFCs are received by the SPS and intelligence requests are routed to CR. CR is the executive agent for the DHS

[11] The creation of a Single Point of Service concept was among the primary recommendations of the I&A sponsored study entitled "Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps"

Intelligence Enterprise RFI system, as specified in DHS Intelligence Enterprise Directive 8310. CR receives, documents, validates, staffs, and processes all intelligence related SLSRs, and coordinates the integration of SLFC intelligence information needs into the Standing and Priority Intelligence Information Needs of the Department.

The RP Reports Officer Program facilitates the reporting of DHS produced or acquired information to the IC, specifically including intelligence analysts at the SLFCs. RP disseminates products to the SLFCs through the HS SLIC restricted portion of the HSIN-Intelligence portal at the controlled, unclassified level and the HSDN portal at the Secret classified level. RP also manages the collection of SLFC-unique information through specific, State-hosted web-pages on HSDN and the HS SLIC-restricted portion of the HSIN-Intelligence portal.

The SLFCs receive analytical products and interacts with intelligence analysts from the three analytic divisions within I&A: Borders and Chemical, Biological, Radiological, Nuclear, and Explosive Threat Analysis (BCTA); Critical Infrastructure Threat Analysis (CITA), the I&A portion of Homeland Infrastructure Threat and Risk Analysis Center (HITRAC); and Homeland Environment Threat Analysis (HETA). These divisions develop products for the DHS stakeholders in their respective areas of expertise, specifically including the SLFCs, as appropriate. These divisions interact with SLFCs in responding to SLSRs and through joint development of products with SLFC analysts. Intelligence analysts from these divisions interact frequently with SLFCs through a wide variety of mechanisms including portal, controlled-unclassified and classified email and phone, and person-to-person visits, and conferences.

Analytic divisions also manage the HS-SLIC, a national community of intelligence analysts focused on homeland security intelligence. Through a restricted portion of the HSIN-Intelligence portal, weekly threat teleconferences at the Controlled Unclassified Information (CUI) level, bi-weekly Secret Video-Teleconferences, and annual national and regional conferences up to the Secret level, the HS SLIC provides a secure forum for the multi-directional sharing of timely, accurate, and actionable information exchange between DHS and SLFCs. The HS SLIC is governed by a steering group representing all the member States.

5.4 Information Management Support

SLFC connectivity to the DHS enterprise is primarily managed by the Information Sharing and Knowledge Management Division (I&A/IM), with the support of OPS and other DHS elements. This connectivity is provided through access to DHS' networks including HSIN-Secret, HSIN-Intelligence, and HSDN, creating an information sharing environment that serves all stakeholders' needs

and builds integration both horizontally and vertically. HSIN is managed and supported by OPS. It provides a portal driven environment to support the exchange of information from DHS to its partners at all levels of government and the private sector. HSIN-SLIC is a restricted portion of the HSIN-Intelligence platform used for the sharing of raw intelligence among community members.

The information exchange standards by which DHS standardizes the flow of information to and from State and locals, including fusion centers, is the National Information Exchange Model (NIEM), a joint DHS, DOJ and Global Justice initiative designed to standardize information exchange. NIEM has been recognized as the exchange standard by the PM-ISE. The Enterprise Data Management Office, in the Office of the Chief Information Officer, is the DHS lead for the implementation of NIEM within DHS.

DHS OCIO also supports fusion centers through development and management of tools available through HSIN. The NOC COP provides a geospatial situational awareness tool via the Integrated Common Analytical Viewer (iCAV) on HSIN. iCAV is a key part of the DHS Geospatial Information Infrastructure (GII). The Geospatial Management Office of the OCIO, in partnership with the DHS Information Infrastructure Collection Division, is responsible for the development and maintenance of the GII.

5.5 Infrastructure Protection Support

To support SLFC analysis and management of risk to critical physical and cyber infrastructures, NPPD coordinates Department-wide activities and plans with those of State, local, tribal, and territorial government partners, and serves as a liaison with the Department for those partners. The DHS mission is to reduce the risk of attack against the nation by protecting critical physical and cyber infrastructure, guarding against threats posed by foreign travelers to the country, and by standardizing the Department's approach to the analysis and management of potential risks to the nation. DHS engages with public and private sector partners to ensure effective information exchange, collaboration, and supervises the development of synchronized doctrines at the national and regional levels.

IP facilitates the identification, prioritization, coordination, and protection of CI/KR in support of Federal, State, local, territorial, and tribal governments, including SLFCs, as well as the private sector and international entities. IP ensures the sharing of risk analysis information and reduction measures to critical infrastructure owners and operators nationwide and across the 18 critical infrastructure sectors. In addition, IP coordinates operational support to government and private entities in response to significant threats and incidents.

Protective Security Advisors

DHS placed Protective Security Advisors (PSAs) in local communities throughout the country to assist with local efforts to protect critical assets. PSAs are located in 40 States and 1 Territory with 10 additional PSAs being added in Fiscal Year 09 so that there will be at least one PSA in all 50 States. PSAs are on-site critical infrastructure and vulnerability assessment specialists, acting as liaisons between DHS and other Federal agencies, State, territorial, local, and tribal governments, and the private sector. As IP's operational field component, PSAs work directly with SLFC representatives, in support of their critical infrastructure security efforts. In many of the SLFCs, PSAs in coordination with SLFC representatives have established a critical infrastructure protection (CIP) Desk. The CIP Desk focuses on real-time situational awareness of nationally significant infrastructure as well as threat integration and coordination, and target and risk analysis. PSAs work closely with SLFCs providing insight to and assistance with the prioritization of critical State and local assets, information sharing and planning efforts, and operational integration.

State Local Tribal and Territorial Government Coordinating Council

In addition, the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC), the State/local cross-sector component of the sector partnership described in the National Infrastructure Protection Plan (NIPP), has direct connectivity to the SLFCs. The SLTTGCC is a forum that is empanelled to identify and inform the coordination between national CI/KR entities and State, tribal, territorial, and municipal officials. The largest representation is from State Homeland Security Advisors (HSAs) and their designated representatives, who are accountable for the development of critical infrastructure protection policies or programs at the State, local, tribal, and territorial level. Partnering with DHS, members of the SLTTGCC share information and provide direction and support to SLFCs.

Homeland Infrastructure Threat and Risk Analysis Center

To support State and locals in understanding the threats and associated risks to critical infrastructure, HITRAC – a joint IP/I&A program – develops analytical products by combining intelligence expertise based on all-source information, threat assessments, and trend analysis with practical CI/KR expertise informed by current infrastructure status and National Infrastructure Simulation and Analysis Center analysis. A key conduit for this information is through the SLFCs.

Office of Cyber Security and Communications

The Office of Cyber Security and Communications (CS&C), also located within NPPD, interacts with SLFCS to ensure the security and continuity of the nation's cyber and communications infrastructures in the event of terrorist attacks and

national disasters. Additionally, CS&C strengthens the reliability, survivability and interoperability of the nation's communications capabilities, including those utilized during emergencies, at the Federal, State, local, tribal, and territorial levels.

US Computer Emergency Readiness Team

The US Computer Emergency Readiness Team (US-CERT), a partnership between DHS and the public and private sectors, coordinates with SLFCs to provide assessments of cyber threats and vulnerabilities to the nation's CI/KR. Established to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. US-CERT continuously assesses and reduces potential damage from such events. During an incident, US-CERT will perform strategic analysis, issue cyber warnings/alerts, and coordinate cyber response and recovery efforts. US-CERT maintains a 24x7 operations center with connectivity to all major Federal cyber operations centers and private sector Internet Service Providers, Information Sharing and Analysis Centers, Sector Coordinating Councils, control system critical infrastructure sector entities, and information technology vendors. In order to foster information sharing and coordination, the Multi-State Information Sharing and Analysis Center will be utilized by US-CERT to coordinate the dissemination of information among the States.

5.6 Domestic Nuclear Detection Support

Nuclear detection information is coordinated between the SLFCs and the Domestic Nuclear Detection Office (DNDO). The Domestic Nuclear Detection Office (DNDO) is a jointly-staffed, national office established to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the Nation, and to further enhance this capability over time. The Joint Analysis Center (JAC) of DNDO serves as the primary conduit between DNDO and the SLFCs for information on radiological and nuclear incidents. The JAC assists State and local entities in situations where a radiation alarm is activated and they require Federal assistance. Also, the JAC acts as a radiological/nuclear technical reach-back center for State or local authorities who have a radiological/nuclear threat, or require technical information on nuclear related materials. The JAC receives information from State and local authorities on potential nuclear threats, problems, or concerns. The JAC participates in the weekly HS-SLIC teleconferences with SLFCs and periodically reviews information posted for SLFCs on the HSIN portal. DNDO is developing a pilot interaction with each State and local agency based on the specific requirements associated with nuclear alarm adjudication. Depending on the state-level alarm adjudication protocols (being defined and implemented by DNDO with each state), the Fusion Center may be part of the alarm adjudication process. The

Fusion Center may be the organization where intra-state and federal organizations share information on ongoing nuclear detection alarms, notify appropriate state and federal agencies, and coordinate any required support and/or response. The JAC will facilitate a working relationship, adjudicating alarms, sharing reports, situational awareness, and assessments through DHS partners in these fusion centers.

5.7 Security Support

The DHS Office of the Chief Security Officer (OCSO) will provide security services in support of the DHS initiatives directed toward State, local, and tribal governments, including the SLFC Program, and the private sector. This support is coordinated through the SLPO to ensure unity of effort and consistency in DHS outreach. OCSO will continue to provide the following security support in support of the SLFC Program:

- Personnel security support including security clearance investigative processing, National Agency Check, adjudication, and reinvestigations.
- Physical security support including guidance on physical security equipment, intrusion detection systems, the conduct of various assessments, Open Storage Certification surveys, etc.;
- Information security (including classification management) support establishing administrative policies and procedures for identifying and controlling information from unauthorized disclosure, classified information, the protection of which is authorized by EO or statute. (In general, classification management encompasses those resources used to identify, control, transfer, transmit, store, retrieve, inventory, archive, and declassify or destroy classified information.);
- Certification of joint occupied facilities, particularly spaces in which SLFCs are collocated within other government agency facilities, that meets both IC and DHS standards, as related to the coordinated of memorandum of agreements and co-use arrangements in advance of DHS operations in a fusion center.
- IT and Communications Security (COMSEC) support that primarily involves the verification and/or certification of existing facilities; granting Open Storage approval; and terminating approvals, documentation and record keeping;
- Support of information sharing policy development governing the sharing of classified national security information with State and local officials and entities and policy and procedures development in support of the SLFC Program;
- Security education, training, and awareness for State and local personnel including initial clearance indoctrination briefing, annual refresher security training, security debriefing(s), and specialized security training, which may include computer security training, courier training, foreign

travel training, and provides COMSEC training, operations security (OPSEC), and counter-intelligence awareness training; and
- Security inquiries and investigations that include security violations, counter-intelligence preliminary investigations, and related law enforcement issues.

The Security Compliance Review Program for SLFCs will include site visits, assessments, and surveys to determine the status of the security program at specific locations and to evaluate its effectiveness. This also includes the identification, tracking, and closure of findings or deficiencies noted in pre-surveys, surveys, or assessments.

OCSO will further support the SLFC mission through the staffing of (6) Field Security Coordinators (FSC). FSCs will be specifically dedicated to supporting the implementation, management, operations, and oversight of State, local, and Tribal security programs, and provide for the unified and consistent application of security standards pursuant to the OCSO *FSC Implementation Plan*, dated February 2008.

5.8 Capability Development Support

As SLFCs are a key element of national preparedness, the FEMA Grant Programs Directorate (GPD) and NPD support SLFCs through four mechanisms: prevention and preparedness grants, technical assistance, training, and exercises. Each of these involves outreach to fusion centers either through DHS structures or collaboratively through the joint DHS-DOJ technical assistance program. GPD and NPD will maintain their current processing patterns and outreach as they interact with SLFCs.

Requests from SLFCs for grants and training information received by any DHS element (including any portions of FEMA) will be forwarded to a central coordination point for tracking and response. This central coordination point will ensure that the SLPO and the NOC Fusion Cell are aware of all interactions for situational awareness. NPD, in conjunction with the DOJ's Bureau of Justice Assistance, will continue to offer technical assistance, exercises, and training, as identified in section 11.1 below.

Other Departmental central coordination points, specifically including the SLPO and the NOC Fusion Cell, will be made aware of current offerings in the form of training and technical assistance. With this awareness, the organizations responsible for the other interactions with SLFCs will be able to make recommendations or identify opportunities that would benefit a specific fusion center.

6.0 DHS Operational Component Coordination

DHS operational component agencies, with law enforcement and/or intelligence missions including, ICE, CBP, TSA, the United States Citizenship and Immigration Services (USCIS), the United States Secret Service (USSS), and the USCG have a significant number of field offices located throughout the United States and have worked closely with their regional, State, and local counterparts on matters of mutual interest for many years. Many of these field offices are located in close proximity to SLFCs, and State, local and regional colleagues are providing information to the field offices that is directly relevant to their mission needs. Many field components have already established relationships with SLFCs and, in some instances, have assigned representatives to the SLFCs.

In order to ensure unity of purpose and a better understanding of and relationship with SLFCs, each DHS component field office whose mission aligns with the priorities of the fusion center will establish a relationship with that center. This relationship should include, but not be limited to, routine meetings and consistent information sharing with DHS and State and local personnel assigned to each center. DHS staff, including intelligence professionals and law enforcement personnel detailed to the SLFCs will share information in accordance with the laws and other authorities governing respective interactions, including Constitutional, statutory, regulatory, and other legal and policy requirements, as appropriate, and all applicable privacy and civil liberties standards.

Additionally, DHS component headquarters and field offices, working in collaboration with I&A, will determine where the detailing of officers or other personnel to the SLFCs is appropriate. Priority is being placed on border fusion centers to ensure compliance with the Act. I&A has created a DHS Fusion Center Integration Working Group, chaired by the SLPO, that is charged with facilitating this initiative. The subsequent decision to deploy personnel and the names of the individuals deployed to the SLFCs will be provided to the SLPO.

TSA will interact with SLFCs through their Federal Air Marshals and TSA Field Intelligence Operations Specialists assigned to Federal Security Directors at major airports. This will build upon programs to place staff in fusion centers. Future deployments will be coordinated with the SLPO. TSA will also coordinate with the fusion centers and respond to requests for information as required.

USCG will interact with SLFCs through Coast Guard field units. These interactions primarily involve matters within Coast Guard jurisdiction in port/coastal areas and may extend to the part-time, temporary, or rotational

assignment of personnel in fusion centers. USCG will continue to coordinate activities within the Department and with Governors, their Homeland Security Advisors, law enforcement partners, critical infrastructure operators, and SLFCs.

ICE will continue to share information with SLFCs on a range of issues, including, but not limited to: tactical information, Organized Crime and Trans-National Gangs information, threat notices, officer safety information, intelligence assessments, commercial intelligence products, open source information, international terrorism, Weapons of Mass Destruction analysis, immigration status, travel records, impact trends, trafficking patterns, and relevant operations that affect State and local law enforcement agencies. Deployment of ICE personnel to fusion centers will be coordinated with other DHS field representatives and with the SLPO.

CBP will interact primarily with SLFCs in border states through CBP field elements or the placement of its Officers, Border Patrol agents, or intelligence analysts in SLFCs. CBP will share information with SLFCs focusing on cross-border related criminal activity, as well as threat notices, officer safety information and intelligence assessments. CBP also coordinates with SLFCs to provide information regarding ongoing CBP initiatives and law enforcement operations. Deployment of CBP personnel to fusion centers will be coordinated with other DHS representatives and the SLPO.

USCIS, in coordination with I&A, will provide centralized information support and will coordinate with SLFCs, law enforcement, and IC requests for immigration documentation and information. USCIS provides subject-matter expertise on immigration and naturalization issues, and is the records custodian of more than 60 million alien files that contain biographical, family, and other data on aliens who seek U.S. immigration benefits. USCIS's Fraud Detection and National Security (FDNS) will facilitate, manage and oversee the sharing of immigration benefit information and the collaboration between USCIS and SLFCs. This USCIS support to SLFCs will be achieved through FDNS Officers who are deployed in USCIS's field offices throughout the United States, and are the Subject Matter Experts for ICE's Immigration Benefit Fraud Task Forces (IBFTFs), as well as local JTTFs and other law enforcement and intelligence agencies.

7.0 Training and Technical Assistance

Training and Technical Assistance for State and Local Personnel
I&A provides an Intelligence Analyst training course for State and local personnel assigned to the fusion centers, entitled "DHS Critical Thinking and Writing Skills Workshop." This course is being offered by mobile training teams

to fusion center staff regionally throughout the country in order to minimize personnel time away from their respective centers.

Additionally, SLFCs may leverage allowable homeland security grant funds to support related training activities of fusion center personnel and analysts. Currently, the following intelligence- and fusion-related courses have been approved for use of DHS grant funds:

- Basic Intelligence and Threat Analysis Course (BITAC), delivered by DHS I&A;
- Analytic and Critical Thinking Skills (ACTS), delivered by DHS I&A;
- Anti-Terrorism Intelligence Awareness Training Program (AIATP) delivered by Federal Law Enforcement Training Center (FLETC);
- Introductory Intelligence Analyst Training Program (ITATP); delivered by FLETC;
- Foundations of Intelligence Analysis Training (FIAT);
- Florida's Law Enforcement Analyst Program;
- Advanced Criminal Intelligence Analysis to Prevent Terrorism (ACIAPT); delivered by National White Collar Crime Center;
- Office of the Director for National Intelligence (ODNI) Analysis 101;
- California's Terrorism Liaison Officer Program; and
- Developing an Intelligence Capacity in State, Local and Tribal Law Enforcement Agencies: A Quick Start Program, delivered by Michigan State University.

Analyst training courses, such as those applicable courses listed above, that leverage DHS grant funds are expected to be in accordance with the Global Justice Information Sharing Initiative's Minimum Criminal Intelligence Training Standards for Law Enforcement.

To facilitate the development of national fusion center capabilities, the DHS FEMA NPD and the DOJ's Bureau of Justice Assistance (BJA) have partnered to develop the Fusion Process Technical Assistance Program. This program has been developed with the support of I&A and in coordination with ODNI, the PM-ISE, the FBI, and experts from the State and local community to include Global, the Global Intelligence Working Group (GIWG), and Criminal Intelligence Coordination Council (CICC).

In an effort to accelerate the implementation of baseline capabilities within all SLFCs, DHS and DOJ have partnered to develop targeted Fusion Process Technical Assistance Services. Each service supports the implementation of the Global Fusion Center Guidelines and the ODNI Information Sharing

Environment Implementation Plan to facilitate the nationwide development and/or enhancement of the fusion process.[12]

Additionally, the NPD National Exercise Division (NED) manages the Terrorism Prevention Exercise Program (TPEP). The TPEP conducts tabletop and live training exercises to regularly assess the capability of individual and regional networks of State, local, tribal, and regional fusion centers. The TPEP has partnered with the DHS/DOJ Fusion Process Technical Assistance Program to coordinate delivery of fusion center exercises and evaluate the effectiveness of technical assistance offerings.

FLETC's Office of State and Local Training (OSL) provides training in anti-terrorism intelligence awareness, intelligence awareness for law enforcement executives, and an introduction to intelligence analysis for SLFC analysts. FLETC interaction with SLFCs is through the delivery of intelligence awareness, analysis, and other related training programs developed for the benefit of the Federal, State, local, tribal, and campus law enforcement community. The FLETC Computer and Financial Investigations Division (CFI) offers financial investigations, computer forensics, and intelligence analysis training to Federal, State, local, campus, and Tribal officers. OSL programs are made available at venues across the United States and are provided tuition-free. OSL also has the capability to extract portions of these programs and offer them at regional training symposia for regional training events. CFI programs are open to State, local, campus, and tribal officers and likewise made available at venues across the United States, and internationally. All of OSL and CFI intelligence related programs comply with guidelines established by the National Criminal Intelligence Sharing Plan.

8.0 Illustrative Use Case: Requests from SLFCs for Information or Support

This section details an illustrative use case of this CONOPS for information or support requested by SLFCs or DHS detailees to SLFCs.

Receive

The fusion center sends a SLSR to DHS and enters the Single Point of Service (SPS) at the NOC Fusion Cell. SLSRs are divided into three types: national, operational, and intelligence. National and operational requirements are specific, time-sensitive/critical, fill information gaps, and require a response as soon as possible. For those requests requiring formal inquiry to the broader IC,

[12] To date the joint DHS/DOJ Fusion Process Technical Assistance Program has delivered more than 100 separate technical assistance services to fusion centers to support their development and implementation of a baseline level of capabilities.

the collection requirements manager within I&A will receive and participate in tracking the requests as documented in DHS Intelligence Enterprise Directive 8310 detailed in Appendix E. Component organizations will be required to provide a response to requests within a stated timeframe.

Review and Route

The request will be reviewed against criteria such as subject matter classification, time sensitivity, evident urgency, and other pertinent quantitative and qualitative factors. Requests will be reviewed and validated to determine the appropriate organization to respond.[13] If the information is related to a current event occurring at the local level, the appropriate personnel of NOC Watch as well as I&A will be immediately notified. If the information is not time sensitive, it will be routed to the appropriate component or entity. For example, if the request is related to an issue on the Mexican border, it will be routed to the appropriate CBP personnel and I&A's BCTA border analysts.

Requests and information will be reviewed and forwarded for possible fusion with other DHS or national intelligence information, as appropriate. Requests and information will also be handled consistent with any applicable security or other information controls, including those associated with investigative case or sensitive law enforcement information, personally identifying privacy data, and U.S. Persons information requiring the application of unique handling and oversight procedures. The tracking log will be updated indicating where the request has been routed and estimated time of completion. At any time during the process the fusion center can request an update on the status of the request.

Respond

Once the request is routed to the appropriate organization, the entity to which the SLSR is assigned processes and responds to the request. For timely event data, the NOC Fusion Cell will follow its established procedures to ensure that the information is incorporated into the NOC COP and that the appropriate DHS component or leadership is notified. IWW will evaluate to determine if additional intelligence can be added to the information. For other types of information, such as intelligence reports or non-time sensitive requests, the receiving entity or the NOC Fusion Cell will forward the request to the appropriate organization for response. The process will facilitate increased collaborative analysis among SLFC analysts and DHS analysts. Any additive information provided by any DHS element will be made available to the NOC Fusion Cell to ensure all have the most current situational awareness.

[13] See Appendix E

The processing component will provide the response back to the fusion center. The fusion center will be responsible for providing the requestor the response. The response will be made visible so that there is a record of how the request has been fulfilled and tracking is completed. If the request is based on information provided by the fusion center, the fusion center will receive feedback indicating the usefulness of the information, how it was combined with other data, and, if possible, any products resulting from or including the information.

9.0 Performance Measures

In order to ensure that DHS support to SLFCs is meeting stakeholder requirements, the SLPO will serve as the designated entity in I&A to capture SLFC customer feedback and to produce a periodic report on that addresses the feedback. So as not to overburden SLFCs, the survey tool will be succinct, consisting of no more than one-page and will be completed by SLFC leaders or the I&A field officers once a quarter. A Project Team, Co-Chaired by the SLPO and PM, will also develop a proposed set of performance metrics that I&A leadership can use to monitor the progress of efforts to upgrade the quality of SLFC support.

In addition, DHS with FBI, as part of the NFCCG, will issue a yearly survey to the Homeland Security Directors and/or SLFCs. The survey results provide an important baseline of fusion center capabilities and indicators of how Federal agencies might better provide support. Any DHS metrics will be coordinated with this interagency process to ensure that consistent metrics are used across the respective entities.

With regard to SLFC capability building, the NFCCG has developed *Baseline Capabilities for State and Major Urban Area Fusion Centers,* a companion document to the *Fusion Center Guidelines*. The document identifies the minimum baseline operational standards for fusion centers. Once implemented, the baseline capabilities will allow for the development of both qualitative and quantitative measures of performance which conform to the Targeted Capabilities List Measures and Metrics. The SLPO, as a partner in the NFCCG, will be responsible for the development of metrics for the overall Federal/SLFC partners. These metrics, as well as all other relevant quantitative and qualitative measures, will also be used in exercises to assess SLFC performance.

10.0 Governance

To ensure compliance with statutory requirements and to effectively manage the SLFC Program, the DHS Information Sharing governance structure will provide consistent oversight of the program for issues of information sharing.

The Information Sharing Governance Board (ISGB) provides a forum for senior DHS intelligence, operational, and management leaders to ensure consistent information sharing governance and management, both internally and externally, and will provide strategic oversight to those DHS information sharing relationships within fusion centers. The ISGB is responsible for ensuring consistency in information sharing and collaboration policy, procedure, and relationships across the Department. The ISGB will serve the functions of the SLFC Council as stated in *The Department of Homeland Security Support Implementation Plan for State & Local Fusion Centers*. The ISGB will assist in key decision-making policies related to DHS support and interaction with the SLFCs. The ISGB will engage components to endorse common philosophy, business rules and guidelines, and where appropriate, to prioritize and synchronize initiatives and adjudicate information sharing issues. The ISGB will have oversight authority over this CONOPS, its future development, and its implementation. The governance structure will also ensure that the program supports the oversight responsibilities and activities of the DHS Office of the Inspector General, those committees of Congress with jurisdiction and oversight over particular SLFC activities, and, as appropriate, Office of General Counsel.

The Information Sharing Coordinating Council (ISCC) is the deliberative coordination body for the ISGB and will serve to address SLFC issues on behalf of the Department, and in support of the ISGB. The ISCC will oversee future changes to the SLFC CONOPS, with ISGB approval. In addition to the operational components of the Department, representatives from the Office of Civil Rights and Civil Liberties (CRCL), the DHS Privacy Office (PRIV), the Inspector General, and the Office of the General Counsel are all members of the ISCC.

11.0 Privacy and Civil Rights and Civil Liberties

CRCL and PRIV have teamed together and are working closely with the SLFC Program to ensure civil rights, civil liberties and privacy are preserved.

Per section 705 of the Homeland Security Act of 2002, as amended, (6 U.S.C. § 345) and 42 USC § 2000ee, CRCL ensures individual rights are preserved within the requirements and context of the homeland security environment, including SLFCs. Section 222 of the Homeland Security Act places authority to "assur[e] that the technologies used by the Department to protect the United States sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information," and to "assur[e] that the Department complies with fair information practices as set out in the Privacy Act of 1974" with the Chief Privacy Officer.

In addition to their organic authorities, the 9/11 Commission Act of 2007, Public Law 110-53, requires CRCL and PRIV to provide policy review and analysis, training, and report on SLFCs. Specifically, the Act requires CRCL to:

- Review operations of SLFCs and establish guidelines for civil liberties policies. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511 (a).
- Provide civil liberties training to all officers, intelligence analysts, and private sector representatives in State, local, regional, and Tribal Fusion Centers. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511 (a).
- Conduct a civil liberties impact assessment (CLIA) of the SLFC Program within 90 days after the enactment of the 9/11 Commission Act of 2007.[1] Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511 (a).
- Conduct a CLIA of the SLFC Program no later than one year after the enactment of the 9/11 Commission Act of 2007. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511 (a).

Similarly, the Act requires PRIV to:

- Review operations of SLFCs and establishing guidelines for privacy policies. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511(a).
- Provide privacy training to all DHS analysts assigned to a fusion center. In addition, PRIV is responsible for ensuring all officers, intelligence analysts, and private sector representatives in State, local, regional, and Tribal Fusion Centers receive adequate privacy training. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511(a).
- Conduct a privacy impact assessment (PIA) of the State, Local, and Regional Fusion Center Initiative within 90 days after the enactment of the 9/11 Act of 2007. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511(a).
- Conduct a PIA of the State, Local, and Regional Fusion Center Initiative no later than one year after the enactment of the 9/11 Act of 2007. Department of Homeland Security State, Local, and Regional Fusion Center Initiative, Sec. 511(a).

CRCL and PRIV have conducted the required CLIA and PIA, respectively. Based on issues identified in these assessments, PRIV and CRCL will work with I&A,

SLPO, and directly with fusion centers to ensure any privacy and civil liberties issues are adequately addressed. The PRIV and CRCL will conduct a subsequent assessment within the year in accordance with the 9/11 Commission Act.

In addition to the initial impact assessments, CRCL and PRIV have already provided four hours of specialized training to DHS intelligence analysts currently assigned to a fusion center, and are prepared to deliver the same training to all intelligence analysts before they are assigned to a fusion center in the future.

CRCL and PRIV have further partnered with the PM-ISE and DOJ BJA to specifically craft training for the State and local representatives serving in fusion centers. Portions relating to privacy will include an introduction to Federal privacy law and policy; the PIA process; the Fair Information Practice Principles; the requirements of the ISE; and other topics identified during a needs assessment phase of development. Finally, the training sessions will stress the importance of States and local employees understanding their own jurisdiction's privacy protection framework. Portions relating to civil rights and civil liberties will include training on civil rights and civil liberties statutes, policies, procedures and protocols; cultural competency; policies against racial profiling; and redress.

In addition, CRCL and PRIV will provide SLFCs with the Privacy and Civil Liberties Implementation Guide for the Information Sharing Environment. The Information Sharing Environment Privacy Guidelines Committee, an interagency body, developed this document, to aid the implementation of the Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines), in accordance with the requirements of the Intelligence Reform and Terrorism Prevention Act (IRTPA) and EO 13388.

Finally, CRCL and PRIV stand ready to assist the program or individual fusion centers to take whatever additional actions are necessary to enhance civil rights and civil liberties and privacy within their operation. The offices will continue to work together and with the fusion center participants to communicate their achievements to the American public, and promote transparency and understanding of this important homeland security mission.

Appendix A – Terms and Concepts

State and Local Fusion Centers (SLFCs)
SLFCs are defined as "a collaborative effort of two or more agencies that provide resources, expertise, and information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity."[14] SLFCs are mutually supporting partnerships with State and local governments (including Tribal and territorial entities) staffed by a team of intelligence, law enforcement, and functional professionals who facilitate the multi-directional flow of timely, accurate, actionable, "all-hazard" information between State, local, Tribal, and territorial entities and the national intelligence and law enforcement communities.[15] Among the activities of SLFCs are those comprising the intelligence cycle (wherein information is collected, integrated, evaluated, analyzed and disseminated). Ideally, the fusion center involves every level and discipline of government, private sector entities, and the public, although the level of involvement varies from one SLFC to another. Fusion centers also vary widely depending on their history, nature, functions and compositions.

Access
The ability and opportunity to obtain knowledge of sensitive information.

All Hazards
An approach for prevention, protection, preparedness, response and recovery that addresses a full range of threats and hazards, including domestic and international terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies. [16]

Chief Intelligence Officer (CINT)
The DHS official who exercises leadership and authority over intelligence policy and programs, in partnership with heads of the DHS components. This person holds the title of Under Secretary of Homeland Security for Intelligence and Analysis.

[14] 9/11 Commission Act of 2007, Sec. 206(a)(2)
[15] HSIC RFI Implementation Plan
[16] NIPP Glossary of Key Terms

Classification Guidance
Any instruction or source that prescribes the classification of specific information.

Classified National Security Information ("Classified Information")
Information that has been determined, pursuant to EO 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Collateral Information
Information identified as National Security Information under the provisions of EO 12958, as amended, but which is not subject to enhanced security protection required for Special Access Program or Sensitive Compartmented Information.

Communications Security (COMSEC)
The communications security systems, services, and concepts that constitute protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of any such communications. COMSEC includes crypto security, emission security, transmission security, and physical security of COMSEC material and information.

Communities of Interest (COI)
A group of organizations with similar organizational functions, knowledge, and characteristics, which share a vested stakeholder interest in homeland security. While multiple COIs may have a stakeholder interest in homeland security, the COIs themselves are divided by asymmetries in knowledge, which DHS seeks to ameliorate through improved intelligence information sharing.

Component
An entity that reports directly to the Office of the Secretary, i.e., the Secretary, Deputy Secretary and his or her staff, and Chief of Staff and his or her staff.

Data Compromise
The access and/or unauthorized disclosure of classified information.

Grants and Training Information
Background and program guidance information to assist auditors in conducting financial audits of grant recipients who receive DHS grant funding.[17] Training is provided by a range of DHS components, including DHS I&A. Grants and training information was previously provided by the DHS Office of Grants and

[17] DHS/FEMA website

Training (G&T), and was transferred to the FEMA Grant Programs Directorate (GPD) and National Preparedness Directorate (NPD), respectively, in April 2007.

Homeland Security Information Network (HSIN)
A DHS enterprise-wide platform designed and implemented to provide secure information sharing among defined communities of interest including Federal, State, local, Tribal, territorial, and critical sector partners.

Information Services Support (ISS)
ISS as an entity in the CR Division of the I&A and is responsible for receiving, documenting, validating, staffing, processing, issuing, tracking, responding, disseminating, and ascertaining customer feedback for RFIs originating from either outside or inside DHS.

Infrastructure Support
Support or access given to SLFCs from DHS in the form of equipment, personnel training, communications systems, hardware, logistics, computers, or funding.

Intelligence Community (IC)
The agencies within the IC, in accordance with applicable United States law and with other provisions, which conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States.

Intelligence Enterprise Policy Directive
A formal written statement by the CINT that: (a) provides authoritative direction on an area of DHS Intelligence policy and (b) does not significantly affect the non-intelligence operations of DHS components.

Interagency Remote Sensing Coordination Cell (IRSCC)
A remote sensing capability/mechanism to coordinate intelligence support for State, local, and Federal Homeland Security communities. This capability represents the contingency (crisis) geospatial intelligence support piece during Incidents of National Significance (INS) where Federal assistance is requested. It is co-located with FEMA's NRCC and the DHS NOC, and is manned by representatives of 12 separate Federal agencies who work to validate, prioritize, and assign remote-sensing (geospatial) requirements.

Investigation Information
Information that is obtained from a variety of sources (e.g. public, governmental, confidential) that may be utilized to further an investigation or could be derived from an investigation.[18]

Request for Information (RFI)
An expression of need within an organization or among organizations for information or production. RFIs can be formal or informal. Formal RFIs can be satisfied by production or collection. Informal RFIs can be satisfied through exploitation of existing information available to DHS. The policies, procedures, and responsibilities for formal RFIs are outlined in DHS' Intelligence Enterprise Policy Directive 8310.19. The individual responsible for validating, staffing, processing, submitting, and tracking of all RFIs originating from both within and outside DHS is referred to as the RFI Manager.

Requestor
The person, component, agency, Community of Interest, or entity that submits a RFI.

Safeguards
Measures and controls that are prescribed to protect classified information.

Security Clearance
A determination made by an authorized Federal agency that a person is eligible for access to classified information. The authorized level of access is determined by the requirements of the position and the type of background investigation.

Security Violation
Any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized access to and/or disclosure of classified information; any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of EO 12958, as amended or its implementing directives; or any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of EO 12958, as amended.

State and Local Support Request (SLSR)
A request for support from state and local entities sent to the DHS NOC Watch Single Point of Service for response.

---

[18] National Criminal Intelligence Sharing Plan Glossary
[19] DHS CIO Intelligence Policy Directive 8310 February 21, 2007

Terrorism Information
The term ``terrorism information'' means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—
(A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
(C) communications of or by such groups or individuals; or
(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Unauthorized disclosure
A communication or physical transfer of information to an unauthorized recipient.

United States Person (US Person)
For purposes of the conduct of Intelligence Activities by elements of the United States Intelligence Community, refers to: "A United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments." [Reference: EO 12333, as amended by EO 13284, Part 3, Sec. 3.4, Subsec. (g) (5) (i)].

Validation
The process to ensure a RFI is appropriately justified. RFIs are considered valid if all of the following conditions are satisfied: (1) the required information is not already available to the requesting organization, entity, or partner; (2) the information is both necessary for, and consistent with, the requestor's organizational mission and need to know, (3) it is technically feasible to obtain the request information; and (4) there is not capability to obtain the requested information using the resources available to the requesting organization, entity, or partner.

Weapons of Mass Destruction
According to the 9/11 Act, "the term `weapons of mass destruction information' means "information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a

terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States."

Appendix B – Acronym List

AMHS	Automated Message Handling System
A&P	Analysis and Production
BCTA	Border and CBRNE Threat Analysis Division
CBP	U.S. Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CFI	Computer and Financial Investigations/FLETC
CFR	Code of Federal Regulations
CICC	Criminal Intelligence Coordination Council
CI/KR	Critical Infrastructure and Key Resource
CINT	Chief Intelligence Officer
COI	Communities of Interest
COMSEC	Communications Security
CONOPS	Concept of Operations
CR	Collection Requirements Division
CRCL	Office for Civil Rights and Civil Liberties
DHS	Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOJ	Department of Justice
EO	Executive Order
FEMA	Federal Emergency Management Agency
FLETC	Federal Law Enforcement Training Center
FSLC	Federal Senior Leadership Council
GCC	Government Coordinating Council
HSIN	Homeland Security Information Network
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HS-SLIC	Homeland Security – State and Local Intelligence Community of Interest
I&A	Office of Intelligence and Analysis
IC	Intelligence Community
ICE	U.S. Immigration and Customs Enforcement
IM	Information Sharing and Knowledge Management Division
IMPT	Incident Management Planning Team
IP	Office of Infrastructure Protection
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
IRSCC	Interagency Remote Sensing Coordination Cell
ISCC	Information Sharing Coordinating Council
ISE	Information Sharing Environment
ISGB	Information Sharing Governance Board
ISS	Information Services Section

IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
IWW	Intelligence Watch and Warning Division
NFCCG	National Fusion Center Coordination Group
NICC	National Infrastructure Coordinating Center
NIPP	National Infrastructure Protection Plan
NOC	National Operations Center
NPD	National Preparedness Directorate
NPPD	National Protection and Programs Directorate
NRCC	National Response and Coordination Center
ODNI	Office of the Director of National Intelligence
OPS	Office of Operations Coordination and Planning
OS	Office of Security
OPSEC	Operations Security
OSL	Office of State and Local Training/FLETC
PCLOB	Privacy and Civil Liberties Oversight Board
PI	Plans and Integration
PIA	Privacy Impact Assessment
PMO	Project Management Office
PRIV	Privacy Office
RFI	Request for Information
RP	Reporting and Production
SINs	Standing Information Needs
SIPRNET	Secret Internet Protocol Router Network
SLFC	State and Local Fusion Center
SLIC	State Local Intelligence Community of Interest
SLPO	State and Local Program Office
SLSR	State and Local Support Request
SLTTGCC	State, Local, Tribal, Territorial Government Coordinating Council
TREP	Terrorism Prevention Exercise Program
TSA	Transportation Security Administration
US-CERT	U.S. Computer Emergency Readiness Team
USCG	United States Coast Guard

Appendix C – Related Interagency Groups

Interagency Threat Assessment and Coordination Group (ITACG)
DHS, with FBI, are leading the ITACG to facilitate the flow of threat information from the IC to State and local governments. The ITACG was established in response to the President's Guidelines for the creation and establishment of the Information Sharing Environment (ISE). Under the recently enacted 9/11 Commission Act, DHS is sponsoring a contingent of State and local law enforcement and homeland security personnel to work as part of the ITACG Detail within the NCTC. This overall effort will enable the development of language to be used within intelligence reports on terrorist threats and related issues that represents the federally coordinated perspective and is tailored to meet the needs of State, local, Tribal, and territorial governments. This coordination of counterterrorism information within NCTC ensures that products released through existing and appropriate channels of the Federal government will be of one voice and without delay. By directly including State and local partners as members of the ITACG Detail, the language appearing in federally disseminated products can be more focused or tailored in areas that are of greater interest and in a form that is most useful to our non-Federal partners.

National Fusion Center Coordination Group (NFCCG)
The NFCCG was created as an activity of the PM-ISE. Specific initiatives are: (1) to define clearly the roles and responsibilities of State and major urban area fusion centers as they relate to the ISE; (2) to define the business processes that support fulfilling that role; and (3) to define how the Federal government can best support the operations of fusion centers. The NFCCG oversees progress with the *DHS/FBI/National Guard Coordinated Deployment Plan*, which is being developed jointly by the FBI and DHS. Its objective is to ensure that both organizations deploy Federal personnel to State and major urban area fusion centers in a coordinated manner. Activities include deployment of DHS personnel to fusion centers, arranging security clearances for those personnel, and accreditation of Sensitive Compartmented Information Facilities at fusion center locations.

Global Justice Initiative (Global)
The Global Justice Initiative is a DOJ-sponsored consortium of Federal, State, local, Tribal, and territorial agencies working to promote information sharing. The Global governance body is the Criminal Intelligence Coordinating Committee which earlier developed and promulgated the 2006 Fusion Center Guidelines. In response to the 9/11 Commission Act, DHS, ODNI, and DOJ have assembled a collaborative fusion center technical assistance program. Among other activities, this initiative holds regional fusion center meetings and is

planning for the next annual Fusion Center Conference scheduled for March 2009. This effort, along with recommendations by the Global Criminal Intelligence Coordinating Committee, has been identified as meeting SLFC technical assistance needs.

National Information Exchange Model (NIEM)
NIEM is designed to develop, disseminate, and support enterprise-wide information exchange standards and process that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation. NIEM is sponsored by DHS, DOJ, and Global Justice and has been adopted for use in the documenting and creating standardized exchanges into and out of the SLFCs. NIEM enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations and data formatted in a semantically consistent manner. NIEM standardizes content (actual data exchange standards), provides tools, and managed processes. NIEM builds on the demonstrated success of the Global Justice XML Data Model as endorsed by Global Justice. Leveraging the successful work of the GJXDM into NIEM, critical exchanges are defined by community stakeholders.

Government Coordinating Council (GCC)
Under the NIPP, a GCC is formed as the government counterpart for each Sector Coordinating Council to enable interagency and cross-jurisdictional coordination for the protection of national CI/KR. The GCC is comprised of representatives across various levels of government (Federal, State, local, or tribal) as appropriate to the security landscape of each individual sector. Cross-sector issues and interdependencies between the GCCs are addressed through the Government Cross-Sector Council and its two sub-councils: the Federal Senior Leadership Council (FSLC) and the State, Local, Tribal, Territorial Government Coordinating Council (SLTTGCC). The FSLC drives enhanced communications and coordination between and among Federal departments and agencies with a role in implementing the NIPP and HSPD-7. The SLTTGCC provides an organizational structure to coordinate across jurisdictions on State- and local-level CI/KR protection, guidance, strategies, and programs; and as such will be a vital informational and operational asset to the SLFCs.

Sector Coordination Council (SCC)
The NIPP sector partnership model encourages CI/KR owners and operators to create or identify an SCC as the principal entity for coordinating with the government on a wide range of CI/KR protection activities and issues. Specific membership will vary by sector, reflecting the unique composition of each sector.

However, membership should be representative of a broad base of owners, operators, associations, and other entities within a sector. The SCCs and their state and regional equivalents will be a vital nexus for SLFCs to and from the private sector.

Appendix D –Authorities

The following table is not inclusive; the authorities contained herein apply to DHS and DHS employees.

Federal Authorities	
Privacy Act of 1974, 5 USC. § 552a, and Computer Matching and Privacy Act of 1988, 5 USC § 552a(b)	The Privacy Act of 1974, 5 USC § 552a (2000), which has been in effect since September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies. It requires that agencies publish notices of their systems of records and sharing of individually identifiable information regarding U.S. citizens and lawful permanent residents subject to certain restrictions.
Homeland Security Act of 2002, as amended	Section 201- Responsibilities of the Assistant Secretary for Information Analysis: To organize, to share, and to obtain law enforcement information with/from Federal, State, and local government agencies.
Intelligence Reform and Terrorism Prevention Act of 2004	DHS shall establish training programs related to terrorist travel intelligence, and enhance public safety interoperable communications at all levels of government.
Implementing Recommendations of the 9/11 Commission Act of 2007	The Secretary, in consultation with the PM-ISE, the Attorney General, the Privacy Officer of the Department, the Officer for Civil Rights and Civil Liberties of the Department, and the Privacy and Civil Liberties Oversight Board shall establish a Department of Homeland Security State, Local, and Regional Fusion Center Initiative to establish partnerships with State, local, and regional fusion centers.
Executive Orders, Presidential Directives, and National Strategies	
Executive Order 12333	Extends powers and responsibilities of US intelligence agencies and directs the leaders of other US Federal agencies to co-operate fully with Central Intelligence Agency (and now the Director of National Intelligence) requests for information.
Executive Order 12958, As Amended, Classified National Security Information	Prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.
Executive Order 12968, Access to Classified Information	Establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.
Executive Order 13231, Critical Infrastructure Protection in the Information Age	Provides for the protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems, in the information age
Executive Order 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security	Outlines responsibilities vested in the Secretary of Homeland Security and takes other actions in connection with the establishment of the DHS. Reflects the transfer of certain functions to, and other responsibilities vested in, the Secretary of Homeland Security, the transfer of certain agencies and agency components to the DHS, and the delegation of appropriate responsibilities to the Secretary of Homeland Security.

Executive Order 13356	Director of Central Intelligence shall set forth common standards for the sharing of terrorism information by agencies within the Intelligence Community in coordination with DHS and State and local authorities.
Executive Order 13388	Agencies shall give the highest priority to counter-terrorism activities and the sharing of terrorism information among Federal, State, and local agencies and appropriate private sector entities.
Homeland Security Presidential Directive – 7 (HSPD-7)	DHS will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations.
Homeland Security Presidential Directive – 8 (HSPD-8)	The Secretary, in coordination with other Federal departments and agencies and State and local governments, will identify relevant classes of homeland-security related information and appropriate means of transmission for the information to be included in an information sharing system.
National Strategy for Information Sharing	All Federal departments and agencies that possess or acquire terrorism-related intelligence and information provide access to such information to NCTC for analysis and integration unless prohibited by law or otherwise directed by the President. As the "Federal Fusion Center" responsible "for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism," NCTC works with appropriate Federal departments and agencies to enable the development of "federally coordinated," terrorism-related information products tailored to the needs of Federal entities. Within the NCTC, the new Interagency Threat Assessment and Coordination Group will facilitate the production of "federally coordinated" terrorism-related information products intended for dissemination to State, local, Tribal, and territorial officials and private sector partners.
Federal Regulations	
6 CFR Part 7 Department of Homeland Security, Classified National Security Information.	Implements Executive Order 12958, entitled "Classified National Security Information," as amended, by establishing the initial elements of the DHS' classified national security information regulations.
28 CFR Part 20 Criminal Justice Information Systems	Applies to all State and local agencies and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated methods where such collection, storage, or dissemination has been funded in whole or in part with funds made available by the Law Enforcement Assistance Administration subsequent to July 1, 1973, pursuant to Title I of this Act.
28 CFR Part 23 et seq. Criminal Intelligence Systems Operating Policies	Instructs that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 USC 3711 are utilized in conformance with the privacy and constitutional rights of individuals.
28 CFR Part 22 Confidentiality of Identifiable Research and Statistical Information	Governs use and revelation of research and statistical information obtained, collected, or produced either directly by Bureau of Justice Assistance, Office of Juvenile Justice and Delinquency Prevention, Bureau of Justice Statistics, National Institute of Justice, or Office of Justice Programs or under any interagency agreement, grant, contract, or sub-grant awarded under the Crime Control Act, the Juvenile Justice Act, and the Victims of Crime Act.
DHS Plans and Directives	

National Infrastructure Protection Plan (NIPP)	NIPP network facilitates two-way and multi-directional information sharing between various security partners through Top-Down Sharing (Federal to local) and Bottom-Up Sharing (local to Federal).
National Response Plan (NRP)	At the Federal headquarters level, incident information-sharing, operational planning, and deployment of Federal resources are coordinated by the Homeland Security Operations Center (HSOC) (now called the National Operations Center/NOC), and its component element, the NRCC. The HSOC facilitates homeland security information-sharing and operational coordination with other Federal, State, local, Tribal, and nongovernmental EOCs.
National Incident Management System (NIMS)	NIMS is a national system that creates standardized incident management processes, protocols, and procedures. NIMS provides a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.
DHS Support Implementation Plan for State and Local Fusion Centers	The SLFC will facilitate effective information flow between the SLFC, DHS components, other Federal partners, and the intelligence community to prevent catastrophic acts such as terrorist attacks.
Safeguarding Classified and Sensitive But Unclassified Information, Reference Booklet for State, Local, Tribal, and Private Sector Programs, U.S. Department of Homeland Security, July 2007	Provides State, local, Tribal, and private sector entities with a reference on the rules for safeguarding classified information and 'sensitive but unclassified' information. It outlines responsibilities upon the granting of a security clearance.
State, Local, and Private Sector Storage And Safeguarding Standards For Collateral Classified Information (State and Local Security Matrix)	Outlines security requirements and standards for State, Local, Tribal, and Private Sector entities for obtaining classified capabilities based on DHS-sponsorship.
Department of Homeland Security, Management Directive 11000, Office of Security	Establishes the responsibilities for the DHS Office of the Chief Security Officer. Its mission is to safeguard the Department's personnel, property, facilities, and information
Department of Homeland Security, Management Directive 11080, Security Line of Business Integration and Management	Establishes the DHS vision and direction regarding the authorities and responsibilities of the leadership of the Department's Chief Security Officer.

Appendix E – The Fusion Process Technical Assistance Program

- Fusion Process Technical Assistance Services
    - Fusion Process Orientation;
    - Fusion Center Governance Structure and Authority;
    - Fusion Center CONOPS Development;
    - Fusion Center Administration and Management;
    - Fusion Center Privacy Policy Development;
    - Fusion Center Technology Technical Assistance;
    - Fusion center and Fire Service Information Sharing and Coordination Workshop;
    - 28 CFR Part 23 Technical Assistance;
    - Fusion Liaison Officer Program Development;
    - Fusion Liaison Officer Program Implementation;
    - State and Local Anti-Terrorism Training;
    - Criminal Intelligence for the Chief Executive;
    - Intelligence Commanders Course;
    - Intelligence Commanders Course;
    - National Information Exchange Model; and
    - Templates and guides for development of privacy and civil liberties policies.
- Fusion Center Fellowship Program
- Fusion Center Exchange Program, which supports the exchange of fusion center personnel and the associated exchange of operational best practices and lessons learned to facilitate the interaction and sharing of information necessary to solidify the national network of fusion centers; and
- Online Fusion Process Resources, including:
    - The Fusion Process Resource Center, located on the Lessons Learned Information Sharing (LLIS) system at www.llis.gov, and
    - The National Criminal Intelligence Resource Center (NCIRC), located at www.ncirc.gov