ANNUAL REPORT TO THE CONGRESS ON THE INFORMATION SHARING ENVIRONMENT

Prepared by the
Program Manager, Information Sharing Environment

This page intentionally blank.

TABLE OF CONTENTS

This page intentionally blank.

EXECUTIVE SUMMARY

Background

In December 2004, Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Section 1016 of IRTPA called for creation of the Information Sharing Environment (ISE).[1;2] Section 1016 also established the Program Manager for the Information Sharing Environment (PM-ISE) with government-wide authority to plan, oversee, and manage the ISE.[3] The Program Manager assists the President and government agencies in the development and operation of the ISE, and monitors and assesses its progress. The law also established an Information Sharing Council (ISC) to advise the President and the PM-ISE on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among Federal departments and agencies (Agencies) participating in the ISE.

To guide efforts to establish the ISE and implement the requirements of IRTPA, on December 16, 2005, President Bush issued a Memorandum to the Heads of Executive Departments and Agencies on the *Guidelines and Requirements in Support of the Information Sharing Environment*. This Memorandum delineated two requirements and five guidelines which prioritize efforts that the President believes are most critical to the development of the ISE and assigned responsibility to relevant Cabinet officials for resolving some of the more complicated issues associated with information sharing. Pursuant to the President's Memorandum, recommendations were developed and submitted to the President on a variety of information sharing related issues including: ensuring the information privacy and other rights of Americans are protected in the development and use of the ISE; improving information sharing with our foreign partners and allies; and establishing a framework for information sharing between and among Federal, State, local, and tribal (SLT) governments and the private sector. These recommendations were submitted to the President and approved for implementation on November 16, 2006.

---

[1] Pursuant to the *Information Sharing Environment Implementation Plan* (November 2006), and consistent with Presidential Guidelines 2 and 3, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA Section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.

[2] The ISE is an approach that facilitates the sharing of information relating to terrorism by putting in place the processes/protocols and technology that enable the sharing of this information among Federal, State, local, tribal and private sector entities, and our foreign partners as well. Creating the ISE is not about building a massive new information system. Rather, the ISE is being established by bringing together, aligning and building upon existing information sharing policies, business processes and technologies (systems), and by promoting a culture of information sharing through increased collaboration.

[3] Recently, the *Implementing Recommendations of the 9/11 Commission Act of 2007*, P.L. 110-53, enacted August 3, 2007, included amendments to Section 1016 of IRTPA and the *Homeland Security Act of 2002*. This Annual Report addresses activities through June 30, 2007, and therefore does not address the new authorities and requirements set forth in P.L. 110-53. New authorities and requirements set forth in P.L. 110-53 will be addressed in subsequent reports.

Section 1016(e) of IRTPA required that the President submit an ISE Implementation Plan (ISE IP) to Congress that included the following:

- A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards;
- A description of the impact on enterprise architectures of participating Agencies;
- A budget estimate that identifies incremental costs associated with designing, testing, integrating, deploying, and operating the ISE;
- A project plan for designing, testing, integrating, deploying, and operating the ISE;
- The policies and directives referred to in subsection (b)(1)(C), as well as metrics and enforcement mechanisms that will be employed;
- Objective, system-wide performance measures to enable the assessment of progress toward achieving full implementation of the ISE;
- A description of the training requirements needed to ensure the ISE will be adequately implemented and properly utilized;
- A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE;
- The recommendations of the Program Manager regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information;
- A delineation of the roles of Agencies that will participate in the ISE; and
- The recommendations of the Program Manager for a future management structure of the ISE.

The President delegated to the Director of National Intelligence (DNI) the ISE IP reporting function set forth in Section 1016(e) of IRTPA. The DNI then submitted the ISE IP to the Congress on November 15, 2006.[4]

This Annual Report to Congress on the ISE is submitted in accordance with requirements set forth in Section 1016(h) of IRTPA. It highlights major accomplishments and areas of significant progress achieved since the ISE IP's delivery, while laying the foundation for long-term management of the ISE.

This Report also documents progress achieved towards initiating, planning for, and designing the ISE, to include:

- Development of proposed Common Terrorism Information Sharing Standards (CTISS). The CTISS program develops and issues *functional standards* that

[4] *Information Sharing Environment Implementation Plan* (November 2006). The ISE IP addresses eleven requirements set forth in Section 1016(e) of IRTPA and describes the actions that the Federal Government intends—in coordination with its SLT, private sector, and foreign partners—to carry out over the ISE's three year implementation timeframe.

document the rules, conditions, guidelines, and characteristics of business processes, production methods, and products supporting terrorism-related information sharing. (Presidential Guideline 1)

- Establishment of a Federally-sponsored interagency capability in the National Counterterrorism Center (NCTC) to enable the production and dissemination of Federally-coordinated, terrorism-related information to SLT authorities and the private sector. (Presidential Guideline 2)
- Establishment of a national, integrated network of State and major urban area fusion centers that optimizes our capacity to better support the information needs of State and local authorities, as well as efforts to gather, analyze, and share locally generated information in a manner that protects the information privacy and legal rights of Americans. (Presidential Guideline 2)
- Development of the *Presidential Guideline 3 Report: Standardize Procedures for Sensitive but Unclassified (SBU) Information.* Currently in interagency review, the Report recommends a new Controlled Unclassified Information (CUI) Framework for rationalizing, standardizing, and simplifying procedures for SBU information in the ISE. (Presidential Guideline 3)
- Development of a repository of information on over 400 unclassified and SBU international information sharing agreements with foreign governments. (Presidential Guideline 4)
- Recognition and adoption of the Critical Infrastructure/Key Resource Information Sharing (CI/KR) framework, established under the National Infrastructure Protection Plan (NIPP) to support the protection and resiliency of the nation's CI/KR, as the private sector component of the ISE
- Presidential approval and PM-ISE publication of ISE Privacy Guidelines. (Presidential Guideline 5) [5]

While capturing the ISE implementation progress to date, this Report will also discuss the challenging task of institutionalizing and ensuring the long-term sustainability of the national information sharing capability needed to protect our communities, our people, and our critical infrastructure from terrorism.[6]

[5] *See* IRTPA Section 1016(h)(2)(A). Section 2.0 of this Report further details "a progress report on the extent to which the ISE has been implemented."

[6] The ISE IP contains 89 specific implementation actions intended to guide planning efforts critical to the establishment of the ISE. It is understood that, as implementation of the ISE progresses and evolves, specific implementation actions defined in the ISE IP will need to be reviewed, re-evaluated, and modified as necessary.

Addressing IRTPA Requirements

IRTPA requires this Report to respond to several specific issues. Response to these requirements is as follows:

Objective system-wide performance goals for the following year.[7]

ISE performance management efforts monitor ISE implementation progress and terrorism-related information sharing performance to enhance mission outcomes, inform investment strategy, and promote accountability. For purposes of measuring progress in establishing the ISE, implementation activities have been organized into four functional areas with corresponding 2008 ISE Performance Goals. These goals provide a target level of performance against which actual achievement can be compared (Table ES-1), as well as a foundation to define target outcomes and results to be accomplished over the next 12 months and beyond.

Table ES-1. ISE 2008 Performance Goals

ISE Functional Areas	2008 ISE Performance Goals
Improving Sharing Practices	Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, private sector, and foreign partners.
Creating a Culture of Sharing	Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.
Reducing Barriers to Sharing	Establish operability that facilitates sharing through a common ISE Information Technology (IT) security framework, to include approved ISE wide Information Assurance (IA) solutions, government-wide physical and personnel security practices, as well as a Controlled Unclassified Information (CUI) Framework across the ISE.
Institutionalizing Sharing	Establish capabilities that allow ISE participants to create and use quality terrorism-related information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for government-wide programs.

An accounting of how much was spent on the ISE in the preceding year.[8]

The PM-ISE used the 2006 Program Reviews to better understand Federal programs, systems, and activities that were considered key to the foundation of the ISE, but not necessarily identified as such. Based on that information, one of the objectives of the 2007 Program Reviews is to identify priorities specific to the ISE and capture an estimate of expenditures, or budget execution dollars. In addition, along with projected Fiscal Year (FY) 2009 through FY2013 expenditures, an investment framework will emphasize specific ISE initiatives to establish associated "baseline" costs for those ISE programs, systems, and activities that are aligned with ISE-related implementation priorities. Future changes in FY expenditures can then be determined in out years, and

[7] *See* IRTPA Section 1016(h)(2)(B).
[8] *See* IRTPA Section 1016(h)(2)(C).

reported in subsequent ISE annual reports. IRTPA authorized the PM-ISE $20 million dollars for FY2007 expenses. These funds, provided from DNI appropriations, supported staff operations, salary, and ISE pilots.

Actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE.[9]

The PM-ISE is currently developing a framework with which to evaluate participating Agencies' ISE-related investments. This framework will be consistent with the Office of Management and Budget's (OMB) principles of program management, and will incorporate a disciplined process to ensure consistent investments in ISE systems and technology. The PM-ISE will establish standardized, repeatable processes that support rigorous analysis of the investment and program-specific data collected. These processes will focus on four ISE Investment Priorities that will help to advance the ISE by FY2009. The initial ISE Investment Priorities include: Suspicious Activity Reporting (SAR) (Presidential Guideline 2), the SBU/CUI Framework (Presidential Guideline 3), the Interagency Threat Assessment and Coordination Group (ITACG)/State and Major Urban Area Fusion Centers (Presidential Guideline 2), and the ISE Shared Space (Presidential Guideline 1). Although these priorities will evolve throughout the life of the ISE based upon ISE mission requirements and stakeholder needs, they will net a first set of improved tangible information sharing capabilities.

The extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors.[10]

Section 4.0 of this Report addresses consistent standards for the consolidated terrorist watch list, known as the Terrorist Screening Database (TSDB), to include the watch listing nomination process, the process for removing individuals from the watch list, and the U.S. Terrorist Screening Center (TSC) process for redress and correcting errors. Due diligence is performed through standardized processes for adding, changing, and removing information in the TSDB, paying special attention to the consolidation of terrorist identity information and the need to protect privacy and civil liberties. These processes, in place since 2004, are designed to address accuracy of the information, its integrity as it flows between organizations, and the appropriateness of information used for watch listing.

The extent to which State, local, and tribal officials are participating in the ISE.[11]

Section 2.0 of this Report summarizes progress made, consistent with Presidential Guideline 2, in implementing a common framework for the sharing of terrorism-related

[9] *See* IRTPA Section 1016(h)(2)(D).
[10] *See* IRTPA Section 1016(h)(2)(E).
[11] *See* IRTPA Section 1016(h)(2)(F).

information between and among Agencies and SLT governments, law enforcement agencies, and the private sector. There has been active participation by SLT government officials in all activities related to the development and design of the ISE. Furthermore, the PM-ISE, in consultation with the ISC, has made significant progress towards improving the sharing of terrorism-related information between and among Federal and SLT governments. This has been done by: (1) establishing a Senior Level Interagency Advisory Group (SLIAG) to ensure effective and immediate implementation of Presidential Guideline 2 recommendations by providing accountability, oversight, and governance; (2) establishing an ITACG Interagency Implementation Team responsible for standing up a Federally-sponsored interagency capability in the NCTC; and (3) establishing a Fusion Center Coordination Group (FCCG) to formalize and coordinate Federal support in the creation of a national, integrated network of State and major urban area fusion centers that facilitates the gathering, processing, analysis, and sharing of terrorism-related information as part of sharing all hazards and all-crimes information at the SLT level. All of these groups have active SLT participation.

The extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to which individuals and organizations outside the government are receiving information through the ISE.[12]

Section 2.0 of this Report summarizes progress made in incorporating private sector data into the ISE. As part of the Presidential Guideline 2 recommendations, the PM-ISE and the ISC agreed, in January 2007, to integrate the CI/KR sector partnership structure, as defined in the NIPP and managed by the Department of Homeland Security (DHS), as the primary private sector coordination mechanism for the ISE. There are also several mechanisms currently in place to facilitate terrorism-related information sharing with the private sector. The ITACG, mentioned above, was established in response to Presidential Guideline 2 to facilitate the production of "Federally-Coordinated" terrorism-related information intended for dissemination to SLT officials and private sector partners. Additional programs and mechanisms that help facilitate the flow of terrorism-related information between the Federal Government and the private sector includes the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the National Infrastructure Coordination Center (NICC), the Protected Critical Infrastructure Information (PCII) Program, and the InfraGard Program.

The measures taken by the Federal Government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals.[13]

Section 5.0 of this Report discusses the accuracy of ISE information. In addition to Privacy Act requirements that apply to Federal Agencies, the ISE Privacy Guidelines require each Agency to establish data accuracy, quality, and retention procedures.

[12] *See* IRTPA Section 1016(h)(2)(G).
[13] *See* IRTPA Section 1016(h)(2)(H).

Moreover, standard security categorization methodologies published by the National Institute for Standards and Technology (NIST) and the Committee on National Security Systems (CNSS) provide additional guidance and direction on how to protect personally identifiable information in information systems throughout the Federal Government. Moreover, as discussed above in the context of terrorism watch lists, special consideration and scrutiny must be applied to information about persons suspected to have a connection with terrorism to ensure that the information is as complete, accurate, and up-to-date as possible.

An assessment of the privacy and civil liberties protections of the ISE, including actions taken in the proceeding year to implement privacy and civil liberties protections.[14]

Section 3.0 of this Report summarizes progress made in implementing Presidential Guideline 5 to ensure the protection of Americans' information privacy and legal rights in the ISE. This includes: (1) delivery and approval of ISE Privacy Guidelines; (2) designation of a senior ISE Privacy Official and establishment of the ISE Privacy Guidelines Committee (PGC) to oversee implementation of the ISE Privacy Guidelines; and (3) establishment of a process, based on the information flow practices of the State and major urban area fusion centers, for ensuring that non-Federal participants in the ISE implement appropriate information privacy policies and procedures that are at least as comprehensive as those contained in the Privacy Guidelines.

An assessment of the security protections of the ISE.[15]

Section 5.0 of this Report addresses ISE security protections to include progress made in implementing the overall risk management methodology and security protection capabilities of the ISE. This progress includes: development of a draft ISE Information Assurance (IA) model; an Information Technology (IT) security and risk management framework; and the establishment of a Memorandum of Agreement (MOA) with the Unified Cross Domain Management Office (UCDMO) to coordinate between the Intelligence Community (IC) and the Department of Defense (DoD) to ensure useful and routine cross-domain solutions (CDS) that allow secure, efficient two-way transfer of information across security classification levels.

[14] *See* IRTPA Section 1016(h)(2)(I).
[15] *See* IRTPA Section 1016(h)(2)(J).

This page intentionally blank.

1 Introduction

1.1 Background and Scope

In the aftermath of the September 11, 2001 terrorist attacks, our nation began the historic transformation aimed at preventing future attacks and improving our ability to protect and defend our people and institutions at home and abroad. Since passage of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), significant progress has been achieved toward establishing an Information Sharing Environment (ISE) that:[16;17]

- Enables greater coordination at the Federal level so that strategic and time sensitive threat information gets into the hands of those who need it to protect our local communities and our nation's interests at home and abroad.
- Makes certain that the Intelligence Community (IC) generates intelligence products that can be quickly shared with those outside the IC such as State, local, and tribal (SLT) entities and our foreign partners and allies.
- Allows the IC to have the means to incorporate into its analytical efforts non-traditional information such as that gathered by law enforcement agencies at all levels.
- Ensures that SLT governments have the capacity to gather, process, analyze and share information and intelligence by establishing an integrated network of State and major urban area fusion centers that communicate, cooperate, and coordinate with each other and with the Federal Government.
- Ensures that private sector data, including information from owners and operators of critical infrastructure, is incorporated into and shared, as appropriate, through the ISE.

[16] Pursuant to the *Information Sharing Environment Implementation Plan* (November 2006), and consistent with Presidential Guidelines 2 and 3, the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA Section 1016(a)(4), as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland. Such additional information includes intelligence information.

[17] Recently, the *Implementing Recommendations of the 9/11 Commission Act of 2007*, P.L. 110-53, enacted August 3, 2007, included amendments to Section 1016 of IRTPA and the *Homeland Security Act of 2002*. The new law expands the scope of the ISE to explicitly include homeland security information and weapons of mass destruction information and sets forth additional ISE attributes. It also endorses and formalizes many of the recommendations developed in response to the President's information sharing guidelines, such as the creation of the Interagency Threat Assessment and Coordination Group, and the development of a national network of State and major urban area fusion centers. This Annual Report addresses activities through June 30, 2007, and does not address the new authorities and requirements set forth in P.L. 110-53. New authorities and requirements set forth in P.L. 110-53 will be addressed in subsequent reports.

This Annual Report to Congress on the ISE is submitted in accordance with requirements set forth in Section 1016(h) of IRTPA. This Report is provided for ISE stakeholders, including Congress and the public, who rely upon the government to improve the sharing of terrorism-related information. The Report describes ISE performance from two complementary viewpoints:

- First, by highlighting major accomplishments and areas of significant progress achieved in implementing the ISE, this Report provides a snapshot of the ISE's evolution to date while pointing out the road ahead to full implementation.
- Second, this Report addresses the development and adoption of plans to effectively manage ISE performance, programs, and investment priorities in subsequent annual reports. The Program Manager for the Information Sharing Environment (PM-ISE), in consultation with the Information Sharing Council (ISC), must ensure that proper management structures are in place to support and maintain the ISE beyond its initial implementation.

1.2 Progress in Implementing the ISE

IRTPA Section 1016(h)(2)(A)

Include "a progress report on the extent to which the ISE has been implemented…"

1.2.1 Key Milestones to Establishing the ISE (Policy)

Executive Orders

On August 27, 2004, the President issued two Executive Orders (E.O.) pertinent to the establishment of the ISE. E.O. 13354 established the National Counterterrorism Center (NCTC) as "the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism [with the exception of] purely domestic counterterrorism information."[18] E.O. 13356 was aimed directly at strengthening the sharing of terrorism information to protect Americans.[19] Specifically, the President directed agencies to give the "highest priority" to the prevention of terrorism and the "interchange of terrorism information [both] among agencies" and "between agencies and appropriate authorities of States and local governments." The President further directed that this improved information sharing be accomplished in ways that protect the information privacy rights and other legal rights of Americans.

IRTPA statutorily established the NCTC within the newly created Office of the Director of National Intelligence (ODNI). IRTPA directed the NCTC to "serve as the primary

[18] Reference E.O. 13354 (August 27, 2004), *National Counterterrorism Center.*

[19] Reference E.O. 13356 (August 27, 2004) *Strengthening the Sharing of Terrorism Information to Protect Americans*. E.O. 13356 was superseded by E.O. 13388 (October 25, 2005) *Further Strengthening the Sharing of Terrorism Information to Protect Americans.*

organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism." Today, the NCTC serves as "the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support." The NCTC strives to ensure that Federal departments and agencies (Agencies), as appropriate, receive and have access to the intelligence necessary to perform their counterterrorism missions.

Designation of the Program Manager

In addition, IRTPA required that the President designate a PM-ISE. The role of the PM-ISE is to manage the ISE, oversee its implementation, assist in the development of ISE standards and practices, and monitor and assess its implementation by Agencies. IRTPA established an ISC to advise the President and the PM-ISE on the development of ISE policies, procedures, guidelines, and standards, and to ensure proper coordination among Agencies participating in the ISE.

Accordingly, on April 15, 2005, the President designated the PM-ISE, and on June 2, 2005, he issued a Memorandum to Heads of Executive Departments and Agencies on *Strengthening Information Sharing, Access, and Integration – Organization, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment,* which directed that the PM-ISE and his staff be located in the ODNI and that the PM-ISE report to the Director of National Intelligence (DNI). On October 25, 2005, the President issued E.O.13388 to facilitate the work of the PM-ISE, expedite the establishment of the ISE, and restructure the ISC.

Guidelines and Requirements

On December 16, 2005, in accordance with Section 1016(d) of IRTPA, the President issued a Memorandum to Heads of Executive Departments and Agencies on *Guidelines and Requirements in Support of the Information Sharing Environment*. The Memorandum prescribed the following guidelines and requirements to support the creation and implementation of the ISE:

- ***Guideline 1***: the President directed that common standards be developed "to maximize the acquisition, access, retention, production, use, management, and sharing of terrorism-related information within the ISE, consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities." These common standards, the President further directed, must accommodate and account for the need to improve upon the sharing of terrorism-related information with SLT governments, and the private sector.
- ***Guideline 2***: the President stressed that the "war on terror must be a national effort" and therefore one in which SLT governments and the private sector are afforded appropriate opportunities to participate as full partners in the ISE.

Accordingly, he directed that a common framework be developed governing the roles and responsibilities of Agencies relating to the sharing of terrorism, homeland security, and law enforcement information between and among Agencies, SLT governments, and private sector entities.

- ***Guideline 3***: the President directed that a series of actions be undertaken to improve upon the sharing of Sensitive but Unclassified (SBU) information. Specifically, he directed the heads of particular Agencies to submit recommendations for the standardization of SBU procedures for marking and handling terrorism-related information, homeland security information, and law enforcement information, and eventually all other types of information shared within the ISE.
- ***Guideline 4***: the President recognized the imperative for the ISE to facilitate and support the appropriate exchange of terrorism-related information with our foreign partners and allies and directed the development of recommendations to achieve improved sharing in this area.
- ***Guideline 5***: the President directed, as he did earlier in E.O. 13353, that the information privacy rights and other legal rights of Americans must be protected. Accordingly, he required that guidelines be developed and submitted for approval to ensure that such rights are protected in the implementation and operation of the ISE.
- ***Requirement 1***: the President directed that the ISE "shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively 'resources') used for the sharing and integration of and access to terrorism information" and shall use those resources to the maximum extent practicable "to establish a decentralized, comprehensive, and coordinated environment for the sharing of such information."
- ***Requirement 2***: the President directed that the heads of Agencies "actively work to create a culture of information sharing within their respective Agencies by assigning personnel and dedicating resources to terrorism-related information sharing, by reducing disincentives to such sharing, and by holding their senior managers accountable for improved and increased sharing of such information."

Submission of the ISE Implementation Plan

On November 16, 2006, and pursuant to the President's delegation of such authority, the DNI submitted to Congress an ISE Implementation Plan (ISE IP). The Report contains descriptions of the functions, capabilities, resources, and conceptual design of the ISE, a plan for deploying and operating the ISE, and a process for measuring implementation progress and performance. Developed by the PM-ISE, in consultation with the ISC, the Report also included the Presidential Guidelines and Requirements and is available on the PM-ISE website (www.ise.gov).

1.2.2 Key Milestones to Establishing the ISE (Operational)

Establishing a fully operational NCTC

The NCTC is a multi-agency organization that serves as the primary organization in the U.S. Government for analyzing and integrating all intelligence possessed or acquired pertaining to terrorism and counterterrorism. It ensures that Agencies have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative, and mission oriented analysis. Authorized Agencies may request information from NCTC to assist in the Agency's activities, consistent with applicable law and guidelines governing access to intelligence. NCTC will enable the sharing of a wide spectrum of terrorism-related intelligence and information among thousands of users in the Federal counterterrorism community through its production of comprehensive, Federally-coordinated, analytical products and the use of its secure web site, NCTC Online (NOL). All Agencies that possess or acquire terrorism-related information provide access to such information to NCTC for analysis and integration unless prohibited by law or otherwise directed by the President.

Creating, within the NCTC, an Interagency Threat Assessment and Coordination Group

Pursuant to Presidentially-approved Guideline 2 recommendations, the Interagency Threat Assessment and Coordination Group (ITACG) will enable the development and production of Federally-coordinated perspectives on intelligence reports and analytical products regarding terrorist threats and related issues that satisfy the needs of SLT partners, and, as appropriate, private sector entities. The ITACG will support the efforts of NCTC to produce Federally-coordinated terrorism-related information products intended for dissemination to SLT officials and private sector partners through existing channels established by Agencies.

Establishing a fully operational U.S. Terrorist Screening Center (TSC)

Established in 2003, the TSC maintains the Terrorist Screening Database (TSDB), the consolidated database for all terrorist identity information. Information on known or suspected terrorists is provided to the TSC by two organizations: (1) the NCTC which provides the TSC with information on known and suspected international terrorists, and (2) the Federal Bureau of Investigation (FBI) which provides the TSC with the identities of known and suspected domestic terrorists who have no link to international terrorism. TSDB information is then made available to Agencies that conduct terrorism screening, including Federal and SLT law enforcement agencies and some foreign governments, for real time searches through data systems that receive real-time or daily updates from TSDB. For example, the TSC has made terrorist identity information accessible through the National Crime Information Center (NCIC) system to law enforcement officers, including 870,000 State and local officers nationwide. TSC also has a 24-hour call center to support terrorist screening processes. The TSDB and the TSC call center

support terrorism screening at Agencies like the State Department (passport and visa applications), the Department of Homeland Security (DHS)/ U.S. Customs and Border Protection (border crossings and international flights), the DHS/ U.S. Bureau of Citizenship and Immigration Services (immigration and citizenship applications), and the DHS/ Transportation Security Administration (domestic flights).

Establishing a national, integrated network of State and major urban area fusion centers

State and major urban area fusion centers are vital organizations and are critical to sharing information related to terrorism. They will serve as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information, while at the same time also handling "all crimes" and "all hazards" related information. Pursuant to Presidential Guideline 2, the Federal Government is promoting the establishment of an integrated network of fusion centers to facilitate effective nationwide terrorism-related information sharing. The Federal Government will support the establishment of these centers and help sustain them through grant funding, technical assistance, and training to achieve a baseline level of capability and to help ensure compliance with all applicable privacy laws. This approach respects our system of federalism and strengthens our security posture. Agencies will provide terrorism-related information to SLT authorities primarily through these fusion centers. Unless specifically prohibited by law, or subject to security classification restrictions, these fusion centers may further customize such information for dissemination to satisfy intra- or inter-state needs. Fusion centers will enable effective communication of locally-generated terrorism-related information to the Federal Government and other fusion centers through the ISE. Locally generated information that is not threat or incident related will be gathered, processed, analyzed, and interpreted by those same fusion centers—in coordination with locally based Federal officials—and disseminated to the national level via the FBI, the DHS, the Department of Defense (DoD), or other appropriate Agency channels. Where practical, Federal organizations will assign personnel to fusion centers and, to the extent practicable, will strive to integrate and collocate resources.

Issuing ISE Privacy Guidelines designed to establish the framework for sharing terrorism-related information in the ISE in a manner that protects the information privacy rights and other legal rights of Americans

In accordance with Presidential Guideline 5, the ISE Privacy Guidelines require Agencies to take actions consistent with core information privacy principles and best practices to: identify information that needs to be protected; assess the legal and policy requirements that apply to that information and applicable sharing arrangements; and put in place the appropriate protections for that information. This framework balances the dual imperatives of sharing information and protecting privacy by establishing uniform procedures for implementing required protections in specific legal and mission

environments. It also establishes an ISE privacy governance structure for de-confliction, compliance, and continuous development of privacy guidance.

Establishing Electronic Directory Services (EDS)

As required in IRTPA Section 1016(b)(2)(G), an interim EDS capability was established to search for and find contact information for watch centers and organizations that have terrorism missions (Blue and Yellow Pages). Capabilities were also delivered to identify terrorism-related information sharing resources (Green Pages) in the Sensitive Compartmented Information (SCI), Secret, and SBU security domains. The ISC determined that the PM-ISE should execute a strategy for increasing the information in the EDS Yellow/Green pages to include entities like fusion centers. The PM-ISE will be working with Agencies to increase contact information in the Blue Pages, as well as to consider the inclusion or establishment of liaison officers where possible and appropriate.

Developing for Release Common Terrorism Information Sharing Standards (CTISS)

Currently under development and pursuant to Presidential Guideline 1, the CTISS program develops and issues functional and technical standards that document the rules, conditions, guidelines, and characteristics of business processes, production methods, and products supporting terrorism-related information sharing.

Establishing a framework to support the sharing of terrorism-related information with our foreign partners and allies

Strong partnerships and trusted collaboration with foreign governments are essential components of the war on terror. Effective and substantial cooperation with our foreign partners requires sustained liaison efforts, timeliness, flexibility, and the mutually-beneficial exchange of many forms of terrorism-related information. The framework was designed, consistent with Presidential Guideline 4, to facilitate the sharing of terrorism-related information with foreign partners by performing the following broad functions:

- Expanding and facilitating the appropriate and timely sharing of terrorism-related information between the United States and our foreign partners;
- Ensuring that exchanges of information between the United States and foreign governments are accompanied by proper and carefully calibrated security requirements;
- Ensuring that information received by Agencies from a foreign government under a sharing arrangement is: (1) provided to appropriate subject matter experts for interpretation, evaluation, and analysis; and (2) can be disseminated and used to advance our nation’s counterterrorism objectives;
- Refining and drawing upon sets of best practices and common standards in negotiating sharing arrangements with foreign governments; and

- Developing standards and practices to verify that sharing arrangements with foreign governments appropriately consider and protect the information privacy and other legal rights of Americans.

2 ISE Stakeholder Community Participation in the ISE

To understand the complexity of the ISE, one needs to realize that it affects the operations of a very large number of Agencies as well as similar governmental entities at SLT levels of government, entities in the private sector, and foreign partners. Each of these stakeholder organizations has a specific focus on terrorism-related information. The ISE is not a new, independent information system. Rather, law and Presidential guidance directs that the ISE must be built upon existing capabilities and resources. The ISE is a system of walkways, skyways, and corridors connecting the homeland security, intelligence, defense, law enforcement, and foreign affairs communities and the users of terrorism-related information within those communities. The objective is to build an ISE that, through common policies, business processes, structure (architecture), and language (standards), will have better, faster, and fuller access to that information because of new or improved walkways, skyways, and corridors.

2.1 Federal-to-Federal Sharing

Achieving improvements in the sharing of terrorism-related information between and among Agencies is the foundation for enabling the Federal Government to better "connect the dots." The Presidential Guideline 2 recommendations propose a framework to govern the roles and responsibilities of Agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of terrorism, homeland security, and law enforcement information as it relates to terrorism, between and among such Agencies.[20] The Presidential Guideline 2 recommendations also include the following descriptions of Federal–to–Federal sharing in each of these areas:

- Acquisition: "Existing authorities provide an ample and appropriate basis to guide the original acquisition of information."
- Access: "At the Federal level, access to homeland security information, terrorism information, and law enforcement information is a function of several factors, including the interoperability of information network architectures, classification authorities and policies, the certification and accreditation of the security of information networks, personnel security requirements associated with sensitive, compartmented information, and the counterterrorism roles and responsibilities assigned to designated organizations. Governance structures are in place to address each of these categories. Accordingly, existing authorities are sufficient to govern access to terrorism-related information at the Federal level."[21]

[20] Presidential Guideline 2 Recommendation Report (approved by the President on November 16, 2006), *Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector*, http://www.ise.gov.

[21] With sufficient existing authorities, the PM-ISE and Agencies can better assess and address the ISE Access Process.

- Retention: "Current retention policies or practices do not appear to impede the sharing of terrorism information."
- Production: "…a coordinated and collaborative approach to production—leveraging the authorized capabilities, focus, and strength of each Agency—is necessary and essential if the Federal Government is going to work effectively with State, local, and tribal officials and private sector entities."
- Use: "At the Federal level, the goal should be to make the maximum amount of information possible available for use by recipients, consistent with applicable law. The National Implementation Plan, as approved by the President in June 2006, sufficiently defines the roles and responsibilities of Federal agencies and departments with counterterrorism obligations."
- Management: "At the Federal level, the management of homeland security information, terrorism information, and law enforcement information is presently inherent in roles and responsibilities articulated in statute, the National Implementation Plan, and agency practice and regulation, all of which impact upon the integration and use of information for analyses and assessment and for the dissemination of intelligence products through the NCTC Online secure web site. A coordinated and shared management approach, one that works effectively with State, local, and tribal officials, is essential to the proposed framework's operational success."
- Sharing: "At the Federal level, NCTC oversees a robust program for the sharing of terrorism information across the Federal intelligence, law enforcement, homeland security, defense, and foreign affairs communities."[22]

Agencies and the PM-ISE are engaged in numerous efforts that enable sharing between and among such Agencies and help meet the Presidential Guideline 2 objectives. In addition to the NCTC and EDS initiatives cited in Section 2.0 of this Report, several other organizational, technical, cultural, and policy Federal-to-Federal information sharing initiatives are described below:

2.1.1 Architecture and Standards

A fully functional ISE requires the construction, integration, and sustained operations of terrorism-related information sharing infrastructures across the Federal Government, SLT governments, the private sector, and foreign partners. During this past year, the PM-ISE introduced the ISE architecture and standards framework, a cross-community, perpetuating framework to help ISE participants adjust, plan, install, and operate current and future information resources that form the infrastructure fabric of the ISE. In compliance with IRTPA and the Presidential Guidelines and Requirements, this framework builds upon processes affecting existing systems throughout the ISE, addresses terrorism-related information sharing across multiple levels of security and

[22] Presidential Guideline 2 Recommendation Report, pages 5-9.

protection levels, and incorporates mechanisms for protecting privacy and civil liberties. This is a long-term approach to information resource planning and management, which also promotes terrorism-related information sharing business process transformation, cultural change, and enhanced performance across the Federal Government and the nation. Agencies have begun to incorporate key elements of the evolving *ISE Enterprise Architecture Framework* (EAF) into their internal efforts to establish or update their internal enterprise architectures. In particular, the Department of Justice (DOJ) has already defined an information sharing segment architecture that will identify and interface agency-wide information sharing architectures into the ISE. Similarly, DHS is also developing a preliminary information sharing segment architecture incorporating ISE attributes. Finally, the Department of State (State) is using the web services model of the *ISE EAF* in its Network Centric Diplomacy system.

The PM-ISE also developed and proposed the CTISS, a common standards framework. The recent development of an initial, nationwide business process and functional standard for suspicious activity reporting is a significant milestone in standards development. This standard, to be implemented as part of an improved Suspicious Activity Reporting (SAR) business process for the ISE, will assist with nationwide integration and information sharing of possible intelligence gathering or pre-operational planning activities related to terrorism, especially across Federal, State, and local levels through State and major urban area fusion centers.

2.1.2 ISE-Wide Education and Training

Presidential Requirement 2 highlights the importance of creating a culture of information sharing among ISE participants. Development of a strong information sharing culture will require both the resources and commitment to improve current sharing practices and policies, and the accountability to ensure that the improvements are implemented. ISE-wide education, training, incentives, and awareness programs, coupled with the detail or exchange of individual Agency personnel, are important parts of this effort.

“Core” awareness training and Agency-specific training are currently under development and review by the ISC Training Working Group. In coordination with the PM-ISE, State’s Foreign Service Institute is currently developing a training course which provides an overview of the ISE. Through Agency-specific training, ISE participants will develop training programs on terrorism-related information sharing, as appropriate, to include integration of the ISE-wide training course into Agency curricula. Furthermore, the ISC Training Working Group will assist DOJ, DHS, and FBI in the development of information sharing training guidelines for use by SLT governments.

2.1.3 Presidential Guideline Three

Lack of a government-wide framework for SBU information severely impedes our nation’s ability to: (1) share information rapidly and confidently so that those that must act have the information they need; and (2) adequately protect sensitive information that

needs to be controlled, and also protect the information privacy rights and other legal rights of Americans. Such a framework for SBU information is essential to facilitate sharing in the ISE and to reduce barriers to sharing. Presidential Guideline 3 requires recommendations to standardize government-wide policies and procedures for SBU.

In 2006, efforts were undertaken under the auspices of a SBU Coordinating Committee (SBU CC) chaired by the PM-ISE to develop the framework. The SBU CC's proposed *Presidential Guideline 3 Report: Standardized Procedures for Sensitive But Unclassified Information* reflects an effort to comply with Presidential Guideline 3 requirements and recommends a new Controlled Unclassified Information (CUI) Framework for rationalizing, standardizing, and simplifying procedures for SBU information in the ISE.

The proposed CUI Framework describes the mandatory policies and standards for designation, marking, safeguarding, and dissemination of all controlled unclassified terrorism-related information, homeland security, and law enforcement information related to terrorism originated by the Federal Government and shared within the ISE. The Framework establishes a simple marking schema that addresses both safeguarding and dissemination that will be used for all CUI. Two levels of safeguarding and dissemination standards will provide necessary protections for CUI, while facilitating its sharing in the ISE. Certain important infrastructure protection agreements between the Federal Government and the Private Sector are not fully accommodated under the current Framework due to additional safeguarding requirements specified in the Framework.[23] As a result, these federal regulations with their associated markings, safeguarding requirements, and dissemination limitations will be "grandfathered" into the CUI Framework. If the President approves the proposed Framework, it is anticipated that an Executive Agent, in coordination with a CUI Council, will govern the new Framework and oversee its implementation.

In addition to this policy and standards guidance, the Report includes a phased, 60-month transition strategy which proposes a planning and implementation approach to transition from the current SBU environment to the new CUI Framework. The report is in the final interagency review process.

2.1.4 Building on Current Capabilities

Adoption of the Critical Infrastructure and Key Resource (CI/KR) Information Sharing framework into the ISE incorporated established interagency structures and processes, such as Government Coordinating Councils (GCC), into the ISE. The GCCs, under the National Infrastructure Protection Plan (NIPP) framework, provide an established structure and process for interagency sharing of strategic and situational homeland security and terrorist information to support the specific mission of CI/KR protection and resiliency within each sector and across sectors. Such structures and processes also

[23] Regulations include *6 CFR Pt. 29 (Protected Critical Infrastructure Information), 49 CFR Pts. 15 & 1520 (Sensitive Security Information), 10 CFR Pt. 73 (Nuclear Regulatory Commission Safeguards Information), and 6 CFR Pt. 27 (Chemical Vulnerability Information).*

incorporate use of a standard set of mechanisms such as the National Infrastructure Coordination Center for notification and information distribution in an emergency. Consequently, the GCCs constitute a formal, standardized method of sharing CI/KR information across the Federal Government.

2.2 SLT Governments

IRTPA Section 1016(h)(2)(F)

Include "the extent to which State, tribal, and local officials are participating in the ISE"

The nature of the transnational terrorist threat and the emergence of homegrown extremists require SLT governments to incorporate counterterrorism activities as part of their daily efforts to provide emergency and non-emergency services to the public. They have now become a critical component of our nation's security capability as both "first preventers" and "first responders," and their efforts have achieved concrete results within their communities. The attacks on our nation crystallized the need to improve the sharing of information to confront the challenges of today's world. We must transform our policies, processes, procedures, and—most importantly—our workplace cultures in order to reinforce sharing as the rule, not the exception, in our efforts to combat the terrorist threat. That means confronting two major challenges:

First – At the Federal level, we must rapidly share information related to terrorism with those who protect our local communities, and we must give it to them in a format that supports the way they do business.

Second – There needs to be an effective process for gathering, analyzing, and when appropriate, sharing locally generated terrorism-related information, and doing so in a manner that protects the information privacy and legal rights of Americans.

Presidential Guideline 2 directed the development of a common framework for sharing information within the Executive branch and with SLT governments, and the private sector. Approved for implementation by the President in November 2006, recommendations contained within the Presidential Guideline 2 Report focus on two principal areas:[24]

1. Establishing, at the Federal level, an interagency capability responsible for coordinating the production and timely dissemination of Federally-coordinated terrorism-related information to SLT authorities, and private sector entities.

[24] In December 2006, the PM-ISE, in consultation with the ISC, established the Senior Level Interagency Advisory Group (SLIAG) to ensure effective and immediate implementation of the Presidential Guideline 2 recommendations by providing accountability, oversight, and governance. Chaired by the Deputy Program Manager, the SLIAG includes membership from: DHS, the DoD, DOJ, FBI, State, the Department of the Interior (DOI), the Department of Energy (DOE), the ODNI, the Central Intelligence Agency (CIA), and the NCTC.

2. Improving collaboration at the SLT level by leveraging State and major urban area fusion centers and by establishing a national, integrated network of these centers.

The Interagency Threat Assessment and Coordination Group

The ITACG is the component within the NCTC that enables and ensures the timely and consistent Federal government-wide coordination of intelligence reports regarding terrorist threats and events that are intended for dissemination to SLT authorities and the private sector. [25;26] As such, the function of the ITACG is critical to the ISE in that it provides the ISE with subject matter expertise necessary to enable informed terrorism-related decision-making at the SLT and private sector levels.

State and Major Urban Area Fusion Centers

As part of the ISE, State and major urban area fusion centers will blend Federal and local information and produce informational products that support the needs of law enforcement and other State and local executives as they develop strategic priorities for their Agencies and, at the same time, produce products that will support the needs of individual police officers, deputy sheriffs, emergency managers, homeland security officials, and others who work with community members to prepare for and prevent crime, violence, and disorder. SLT officials were integral to developing the Guideline 2 Report recommendations approved by the President. Those recommendations represent a common (Federal, State, local, and tribal) view of the role fusion centers will play in the ISE. Furthermore, incorporation of State and major urban area fusion centers into the ISE recognizes that these centers support day-to-day crime control efforts and other critical public safety activities.

Over time, networking these centers will create a comprehensive national capacity to gather, process, analyze, and share information. Incorporating these centers into the ISE will be done in a manner that protects the information privacy rights and other legal rights of Americans. Significant progress has been achieved in implementing the recommendations approved by the President, including:

1. An interagency Fusion Center Coordination Group (FCCG) has been established. Co-chaired by DHS and the FBI, this group, with the full participation of State and local officials, is responsible for ensuring that the Federal Government's efforts to work with State and major urban area fusion centers are coordinated and carried out in a manner consistent with the President's direction.

[25] In December 2006, an ITACG Implementation Team was established. Co-chaired by DHS and the FBI, ITACG Implementation Team membership also included representatives from: DoD, DOJ, NCTC, ODNI, the PM-ISE, Global Justice Information Sharing Initiative (GLOBAL) Criminal Intelligence Coordinating Council (CICC), Major Cities Chiefs, International Association of Chiefs of Police (IACP), National Sheriff's Association, and National Governor's Association Homeland Security Advisors Council.

[26] As of the date of this Report, the ITACG has been established at the NCTC. The ITACG is based on a concept of operations plan developed through a collaborative effort involving Federal, State, and local officials. The PM-ISE has provided funding to offset initial operational costs. A process has been established for selecting State and local personnel for assignment to the ITACG.

2. DOJ and DHS are working together to ensure that relevant Fiscal Year (FY) grant programs prioritize efforts to establish fusion centers (first done for FY2007).

3. DOJ and DHS have broadened the allowable expenses under these programs to address concerns raised by State and local officials.

4. DOJ and DHS have jointly established and are managing the "DHS/DOJ Fusion Process Technical Assistance Program" which provides training to State and local officials on topics such as governance, fusion center management, and privacy policy development. This technical assistance has already been provided to 10 jurisdictions with another 13 jurisdictions to receive it by the end of April 2007, and is available upon request.

5. FBI and DHS are developing an integrated deployment plan to ensure both organizations deploy Federal personnel to State and major urban area fusion centers in a coordinated manner.

6. An ISE Privacy Guidelines Committee has been established to ensure that incorporating fusion centers into the ISE will be done in a manner that protects the information privacy rights and other legal rights of Americans.

Participation of State, local, and tribal officials in planning for and establishing the ISE

There has been active participation by SLT government officials in all activities related to the development and design of the ISE. The ISC established a SLT Subcommittee to provide input regarding the needs and capabilities of SLT and SLT representatives were actively involved in drafting the ISE IP. Representatives also are involved in ISE-related working groups focused on implementing the ISE to include those pertaining to establishing: a government-wide framework for SBU information; a comprehensive framework to govern the gathering and analysis of SARs; the ITACG; a national, integrated network of State and major urban area fusion centers; and CTISS.

2.3 Private Sector

IRTPA Section 1016(h)(2)(G)

Include "the extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to which individuals and organizations outside the government are receiving information through the ISE"

As mentioned above, Presidential Guideline 2 required the development of a framework for sharing information at all levels of government and with the private sector to ensure that private sector data, including information from owners and operators of critical infrastructure, is incorporated into and shared, as appropriate, through the ISE. As part of Presidential Guideline 2 recommendations, the PM-ISE and the ISC agreed in January 2007 to leverage the CI/KR sector partnership structure, as defined in the NIPP and managed through DHS, as the primary private sector coordination mechanism for the ISE.

This coordination mechanism constitutes what was previously referred to as the Private Sector Subcommittee of the ISC and allows for the inclusion of all appropriate private sector or government participants as needed. Specifically, the Critical Infrastructure Partnership Advisory Council (CIPAC) is the primary mechanism through which this coordination takes place. The CIPAC facilitates decision-making across Federal, SLT government, and private sector partners to support ISE-related policy, strategy, plans, issues, and requirements development. At any given time, the CIPAC membership may consist of the CI/KR owner and operator members of various Sector Coordinating Councils (SCC) and the corresponding Government Coordination Councils (GCC), as defined in the NIPP, as well as any other public or private sector entities that are identified to participate in its deliberations. Leveraging the CI/KR in particular, the CIPAC mechanism allows for alignment of the NIPP, the ISE IP, and Presidential Guideline 2. The CIPAC coordination mechanism has already helped shape Presidential Guideline 3 recommendations on standardizing government-wide procedures for SBU information, and is being engaged to focus on further private sector participation in Presidential Guideline 2 activities.

There are several existing mechanisms to facilitate terrorism-related information sharing with the private sector. The ITACG, mentioned above, was established in response to Presidential Guideline 2 to facilitate the production of "Federally-coordinated" terrorism-related information intended for dissemination to SLT officials and private sector partners. Other mature programs and mechanisms that help facilitate the flow of terrorism-related information between the Federal Government and the private sector include the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), the National Infrastructure Coordination Center (NICC), the Protected Critical Infrastructure Information (PCII) Program, and the InfraGard Program.

Guideline 2 calls for production of a plan that implements elements of the framework as it affects the private sector. A baseline document has been developed that supports three levels of decision-making and action: (1) strategic planning and investment; (2) situational awareness and preparedness; and (3) operational planning and response.[27] The paper notes that most of the information shared day-to-day with the CI/KR ISE consists of information necessary for coordination and management of risks resulting from natural hazards and accidents. Consequently, for terrorism-related information sharing to be efficient and sustainable for the CI/KR owners and operators, the same environment must be used for sharing terrorism-related information, homeland security information, and law enforcement information related to terrorism. This baseline document will serve as a roadmap for improved private sector integration into the ISE.

2.4 Foreign Partners

In 2006, the interagency Foreign Government Information Sharing Working Group (FGISWG), chaired by State, submitted the Guideline 4 recommendations to the President to support and facilitate appropriate information sharing between Executive branch departments and foreign partners and allies.[28;29] The PM-ISE also identified actions in the ISE IP that incorporate and set a timeline for implementing certain Presidential Guideline 4 recommendations through June 2009. In response, the FGISWG completed recommendations on foreign information sharing and privacy-related topics and has developed a checklist of issues that Agencies can consider when negotiating international agreements, which is in the final stages of review. State and the PM-ISE are also developing a strategy to encourage bilateral and multilateral efforts among Agencies, whenever feasible and appropriate, to develop "best practices" on terrorism-related information sharing with foreign partners.

In a related effort, the PM-ISE is building a Federal government-wide repository of information that contains, among others, international agreements and information on foreign marking and handling regimes. Comprehensive details on over 400 unclassified and SBU international agreements have already been collected and analyzed for archiving in the repository. This initial operating capability of the repository will provide a needed resource catalog for use by Agencies and enable them to search and locate information relevant to international agreements. Subsequent efforts will include collecting and incorporating classified international agreements, information on foreign government and international organization marking and handling regimes, and the text of any relevant best practices and protocols in the repository.

Several specific initiatives are also underway to improve sharing with foreign partners. State's Consular Affairs Bureau has co-chaired an interagency working group with the

[27] *The CI/KR Information Sharing Environment*, Department of Homeland Security, Office of Infrastructure Protection, April 2007.
[28] *See Presidential Guideline 4 – Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners*, http://www.ise.gov.
[29] Presidential Guideline 4 excluded from the working group's consideration and recommendations those activities conducted pursuant to Sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.

Homeland Security Council to develop an implementation strategy and a draft model agreement for sharing terrorist screening information with foreign partners. In coordination with the TSC, State has several pilot exchanges and has negotiated and signed agreements for terrorism-related information sharing with several foreign partners. State is also actively engaged in establishing information sharing agreements with allied foreign partners and international organizations. This includes a recent agreement with the European Union (EU) on efforts to share classified information.

3 Protecting the Information Privacy Rights and Other Legal Rights of Americans in the ISE

IRTPA Section 1016(h)(2)(I)

Include "an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections"

Progress associated with protecting information privacy rights and other legal rights of Americans in the ISE is fundamental to ensuring the success of future terrorism-related information sharing efforts and creating a culture of information sharing. Both IRTPA and Presidential Guideline 5 highlight this priority. This section explains the mechanisms in place to ensure information privacy protections in the ISE and notes actions taken in the proceeding year to implement or enforce such protections.

In accordance with Presidential Guideline 5, the Attorney General and the DNI, in coordination with the PM-ISE and the heads of Agencies, developed ISE Privacy Guidelines that have been approved by the President.[30] These guidelines call for Agencies to comply with current laws, regulations, and policies related to information privacy and other legal rights. They also put in place internal policies and procedures under a uniform government-wide framework to identify and protect information about Americans that may be shared as part of the ISE, so that it is accessed, used, and retained consistent with the authorized purpose of the ISE and the need for information privacy and other legal protections. Established by the ISE Privacy Guidelines, the ISE privacy governance structure recognizes the difficulty of being able to predict in advance what information an Agency will want to share, in what form, with what other entities, and under what circumstances, and therefore acknowledges that legal and policy protections cannot be predetermined for all sharing arrangements.

Since the release of the ISE IP, considerable progress has been made in implementing the ISE Privacy Guidelines. Each ISC Member Agency designated a senior ISE Privacy Official and the PM-ISE established the ISE Privacy Guidelines Committee (PGC). The PGC includes six working groups organized around: (1) modeling the privacy policy implementation process; (2) training and outreach; (3) SLT privacy guideline implementation; (4) privacy and legal issues; (5) civil liberties; and (6) foreign partners.

The PGC also established a process, based on the information flow practices of the State and major urban area fusion centers, for ensuring non-Federal participants in the ISE implement appropriate privacy policies and procedures which are at least as comprehensive as those contained in the Privacy Guidelines. The process will result in guidance to the fusion centers regarding policies, practices, and procedures for ensuring compliance with the Privacy Guidelines.

30 The ISE Privacy Guidelines can be found on the Office of PM-ISE website, www.ise.gov.

Furthermore, an assessment has been completed of the information privacy and other protections to be afforded by the ISE. Based on a survey of constitutional, statutory, and regulatory authorities as they relate to privacy concerns, and a review of an extensive set of applicable legal authorities, the assessment provides a baseline of information to be incorporated into the implementation process.

In addition to responding directly to ISE IP actions, the PGC is developing: (1) a Definitional Scope document to assist ISE Privacy Officials in identifying the databases and systems within their Agencies subject to ISE Privacy Guidelines; (2) a Model Privacy Policy Implementation Process (MPPIP) and an approach to developing a companion set of tools and guides to assist Agencies in the implementation of the Privacy Guidelines; and (3) Draft Privacy Act guidance for PGC members.

The MPPIP is a step-by-step guide designed to help each ISE privacy official implement the guidelines from start to finish. It will be supplemented by specific tools and guides covering particular topics of common concern, such as:

- A privacy sharing assessment that includes a legal analysis, flowchart, and checklist to help Agencies identify which systems and sharing arrangements fall under the ISE and determine whether “protected information” is involved in those systems; and
- Model privacy policies for data quality, accuracy, and retention.

The PGC is working with Agencies to conduct a review of systems identified as being covered by the ISE and will undertake a training effort of Agency privacy officials and systems’ operators to help them use the MPPIP and Toolkit to implement the ISE Privacy Guidelines for identified systems. Additionally, the PGC is in the final process of developing a recommended policy on Privacy Act routine uses.

4 Consistent Standards for Terrorism Watch Lists

IRTPA Section 1016(h)(2)(E)

Include "the extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors"

The TSC has compiled all identifying information about known and suspected terrorists into a single integrated and consolidated terrorist watch list, known as the TSDB. The TSC makes TSDB data available to Agencies that screen for terrorism through a variety of means. First, many Agencies have access to TSDB data through existing data systems, such as the National Crime Information Center (NCIC), the Treasury Enforcement Communications System (TECS), and the Consular Lookout and Support System (CLASS). Agencies are also able to provide data directly to the TSC for screening against the TSDB and resolution of any potential matches. Finally, the TSC is in the process of deploying the capability for Agencies to perform direct queries against the TSDB through a remote query system.

Consistent standards exist for placing individuals on and removing them from the TSDB. TSDB includes identifying information about "individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism." The TSC enforces that standard by reviewing each and every nomination to add an individual to the TSDB to ensure there is a terrorism nexus. The TSC routinely rejects nominations that do not meet the criteria.

The overall process by which individuals are removed from TSDB is similar to that by which individuals are added to the system. The determination that an individual possesses no nexus to terrorism is primarily left to the nominating Agency or Agencies that originally provided information on the individual. Once a decision is made to remove an individual's record from TSDB, it sets in motion the removal of the individual from all other data systems to which the TSDB record had previously been sent.

One of the TSC's highest priorities is to ensure the TSDB is accurate, current, and thorough. To that end, in January 2005, the TSC established a watchlist redress process to provide for timely and fair review of individuals' complaints, and to identify and correct any data errors, including errors in the terrorist watchlist itself. The TSC redress process is carried out by an independent unit within the TSC that follows written procedures to receive, track, and research watchlist-related complaints, to consult with Agencies that nominate individuals to the watchlist, and to correct the watchlist or other data that was causing an individual unwarranted hardship or difficulty during a screening process. The redress process begins with the screening Agency that receives a complaint from an individual concerning a negative experience during a terrorism

screening process. If the redress matter cannot be resolved locally, it is referred to the TSC's Redress Unit for resolution.

In addition to the watchlist redress process, TSC has several other ongoing quality assurance efforts that seek to identify and correct data errors and inconsistencies in TSDB records. In addition to the nomination review described above, the TSC also conducts Encounter Driven Quality Reviews on records that are the subject of a possible watchlist match during screening; Special Project Reviews, such as the recent review of all records on the No Fly List; and the Record-By-Record Review Project, which will examine all records that have not been reviewed or modified for more than two years.

Upon identification of a quality assurance issue, TSC analysts investigate the details of the issue, determine whether any inaccuracies and/or inconsistencies exist among the data in the records, and identify the origin of any such errors. The analysts then coordinate with the appropriate upstream data providers and downstream screening Agencies to ensure that any necessary corrections can be made to the records in question and propagated throughout the screening community.

Due diligence is performed through standardized processes for adding, changing, and removing information in the TSDB, paying special attention to the consolidation of terrorist identity information and the need to protect the information privacy and other legal rights of Americans. These processes, in place since 2004, are designed to address accuracy of the information, its integrity as it flows between organizations, and the appropriateness of information used for watch listing.

5 An ISE Trusted Environment with Security Protections

IRTPA Section 1016(h)(2)(H) and Section 1016(h)(2)(J)

Include "the measures taken by the Federal Government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals" and "an assessment of the security protections used in the ISE"

The ISE aims to "facilitate the establishment of a *trusted partnership* among all levels of government, the private sector, and foreign partners."[31] This concept of "trust" underlies many of the real or perceived barriers to effective information sharing. To freely share terrorism-related information, and to create a culture of information sharing, ISE participants need to be assured that other organizations will protect the information with an equivalent set of security and access controls. Moreover, ISE participants—as well as Congress and the American people—must be confident that terrorism-related information is as accurate as possible (recognizing the inherent ambiguity of some sources of this information), and that there are adequate processes in place to correct inaccuracies when they arise. This section - responding to the ISE priority area on reducing barriers to sharing - describes preliminary steps taken to improve the accuracy of ISE information and to establish a uniform security framework, two major aspects of the foundation for the trusted partnership envisioned for the ISE.

5.1 Accuracy of ISE Information

IRTPA requires the first annual report to include an update on measures taken to ensure the accuracy of ISE information, in particular information about individuals.[32] In addition to Privacy Act requirements that apply to Agencies, the ISE Privacy Guidelines require each Agency to establish data accuracy, quality, and retention procedures. Moreover, standard security categorization methodologies published by National Institute for Standards and Technology (NIST) and the Committee on National Security Systems (CNSS) provide additional guidance and direction on how to protect personally identifiable information in information systems throughout the Federal Government. In addition, as discussed above in the context of terrorism watch lists, special consideration and scrutiny must be applied to information about persons suspected to have a connection with terrorism to ensure that the information is as complete, accurate, and up-to-date as possible.

5.2 Assessment of ISE Security Protection

Section 1016(h)(2)(J) of IRTPA requires that this Report provide an assessment of the security protections used in the ISE. The ISE is a "decentralized, distributed, and

[31] *See* ISE IP, p.12.
[32] *See* IRTPA Section 1016(h)(2)(H).

coordinated environment," and as such, its overall risk management methodology and security protection capabilities depend heavily on the features and assurance provided by systems designed and operated by participants in all five ISE communities. Given this, a traditional vulnerability and risk assessment of the hundreds of such individual systems—some operating at multiple security levels—would be neither practical nor productive. Instead, the problem is approached by first outlining top-level ISE security requirements that recognize this dependence on individual ISE participants. The resulting strategy is founded on two premises:

- Developing a unified risk management and Information Technology (IT) security framework that will serve all five ISE communities;[33] and
- Increasing the utility and availability of cross-domain solutions (CDS) that allow for secure and efficient two-way transfers of information across security classification levels.[34]

The development of a common ISE IT security framework is linked to the *ISE EAF* framework and profile described in Section 2.0. As part of this effort, the PM-ISE reviewed functional security requirements with the National Security Agency (NSA), NIST, the Assistant Director of National Intelligence/Chief Information Officer (ADNI/CIO), and the CNSS. These requirements were then used to develop a draft ISE Information Assurance (IA) model and IT security and risk management framework that are currently being reviewed and revised. When complete, they will form the foundation for the more extensive follow-on work to be done next year.

In implementing the IT security framework, the ISE will heavily leverage the groundbreaking work done this year by the ADNI/CIO and the Assistant Secretary of Defense for Networks and Infrastructure Integration to streamline and standardize the process for certifying and accrediting IT systems. This effort is addressing a range of IT security issues with the goal of full Certification and Accreditation (C&A) reciprocity across the IC and DoD. In turn, the PM-ISE and ISC Member Agencies will build on this effort to achieve a comparable degree of C&A reciprocity across all Agencies participating in the ISE.

The PM-ISE has established a Memorandum of Agreement (MOA) with the Unified Cross Domain Management Office (UCDMO) that puts into place a coordination process between the IC and DoD to ensure the utility and availability of CDS. This allows for secure and efficient two-way transfers of information across security classification levels.

FY2008 activities will build on this year's work on the common IT security framework and CDS. The priority will be the development and adoption of a common IT security

[33] *See* ISE IP, p. 47-49.
[34] *See* Ibid., p. 50.

framework for the ISE by the State, DoD, DOJ, DHS, and ODNI Chief Information Officers (CIO), consistent with existing policies and procedures.

5.3 Personnel Security Practices

Improved terrorism-related information sharing relies on consistent personnel security practices government-wide with respect to personnel security investigations, adjudication, and reciprocal recognition. Section 3001 of IRTPA called for the President to select a single executive branch element to be responsible for directing day-to-day oversight of the investigations and adjudications of personnel security clearances government-wide, including those for highly sensitive programs. Among other requirements, IRTPA further mandates the development and implementation of uniform and consistent policies and procedures; the reciprocal recognition of access to classified information among the Agencies of the U.S. government; and to the maximum extent practicable, the availability of sufficient resources in each organization to enhance clearance and investigative programs.

Most policies and processes for personnel clearances, re-investigation, and reciprocal recognition lack uniformity, consistency, and trust. Agencies often do not recognize clearances granted under the authority of another Agency, and no central database exists to verify an individual's clearance. This greatly inhibits individuals from working across Agency lines even when their jobs require it.

To remedy these issues, the Office of Management and Budget (OMB) and the National Security Council (NSC) are taking a closer look at government-wide personnel security practices in an effort to propose solutions that align investigations for security clearances with those for employment suitability. This process will proceed through a Security and Suitability Investigations Working Group, chaired by the Office of Personnel Management (OPM). In addition, OPM is completing an extensive analysis of all systems involved in the investigation and adjudication process. The findings will provide insight for a modernization plan across the Federal Government and will improve ISE participants' ability to access and share terrorism-related information.

5.3.1 Certification and Accreditation Practices

The ADNI/CIO and the DoD CIO have announced their intention to transform the C&A process for both the IC and the DoD. The transformation effort will develop and implement shared C&A processes throughout both communities. These proposed changes will strengthen the ability for the IC and DoD to rapidly deploy information technology systems. They will also drive decision-making based on sound risk management principles, incorporate security into common lifecycles that are approved and used by all IC and DoD enterprises, and eliminate wasteful and redundant processes and paperwork. This will ensure that C&A results are accepted across the IC and DoD.

6 ISE Performance Goals

IRTPA Section 1016(h)(2)(A) and 1016(h)(2)(B)

Include "…how the ISE has fared on the performance measures and whether the performance goals set in the preceding year have been met" and "objective system-wide performance goals for the following year"

ISE performance management efforts monitor ISE implementation progress and terrorism-related information sharing performance to enhance mission outcomes, inform investment strategy, and promote accountability. For purposes of measuring progress in establishing the ISE, implementation activities have been organized into four functional areas with corresponding 2008 ISE Performance Goals.[35] These goals provide a target level of performance against which actual achievement can be compared (Table 6.0-1), as well as the foundation to define target outcomes and results to be accomplished over the next 12 months and beyond.

Table 6.0-1. ISE Priority Areas and 2008 Performance Goals

ISE Functional Areas	2008 ISE Performance Goals
Improving Sharing Practices	Establish a set of activities and strategic approaches to facilitate sharing among all levels of government, the private sector, and foreign partners.
Creating a Culture of Sharing	Develop a shared set of values that change behavior of ISE participants through established training programs, trained personnel, incentive programs, and privacy protections among ISE participants.
Reducing Barriers to Sharing	Establish operability that facilitates sharing through a common ISE Information Technology (IT) security framework, to include approved ISE wide Information Assurance (IA) solutions, government-wide physical and personnel security practices, as well as a Controlled Unclassified Information (CUI) framework across the ISE.
Institutionalizing Sharing	Establish capabilities that allow ISE participants to create and use quality terrorism-related information by improving business processes, developing a common enterprise architecture framework, refining common standards, and instituting effective resource management for government-wide programs.

As the ISE matures, future reports will place greater emphasis on the broader, more integrated, and longer-term view of ISE performance management across three perspectives:

Perspective 1: Progress Against ISE Implementation. Progress against ISE implementation can be described in three ways: (1) Intra-agency progress; (2) Interagency progress; and (3) Cross-ISE progress. Over the next 12 months, the PM-ISE, in consultation with the ISC, will continue to measure implementation progress and will report on performance in the June 2008 Report.

[35] *See* IRTPA Section 1016(h)(2)(A) and 1016(h)(2)(B). The ISE Performance Management Approach will allow the PM-ISE, in future annual reports, to document how the ISE has fared on the performance measures and whether the 2008 ISE Performance Goals have been met.

Perspective 2: Information Sharing Outcomes. The PM-ISE, in consultation with the ISC, will begin to measure the outcomes of an operational ISE as it becomes a critical tool in our nation's ability to combat terrorism.

Perspective 3: Institutionalize ISE Performance. To institutionalize performance management in the ISE, the PM-ISE, in coordination with OMB, will focus on the four functional areas to develop measurements. The PM-ISE will then apply these measures to better inform Federal ISE resources decisions.

Successful ISE performance management is a shared responsibility of all ISE participants. Participants must understand what is required, provide the necessary resources, and accomplish the priority tasks to achieve the stated goals of the ISE.

7 ISE Investments

IRTPA Section 1016(h)(2)(C) and 1016(h)(2)(D)

Include "an accounting of how much was spent on the ISE in the preceding year" and "actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE"

Development and growth of the ISE depends on a plan to identify and justify required programs and projects government-wide that will form the foundation of the ISE. It establishes standardized ISE management practices and a trusted partnership among ISE stakeholders.

7.1 2006 Budget and Program Reviews

In August 2006, the PM-ISE and OMB developed cross-cutting budget guidance for ISC Member Agencies to justify funding requests for major IT and other investments supporting the ISE—in whole or in part—for FY2008. In October and November of 2006, the PM-ISE, in coordination with OMB, built on this guidance and conducted ISE Budget and Program reviews of ISC Member Agency terrorism-related information sharing capabilities. The goals of these reviews were to: (1) gain a better understanding of, and begin to establish support for, the programs, systems, and initiatives that form the foundation of the ISE; and (2) identify potential opportunities to leverage current ISE capabilities.

7.2 Approach for Influencing Outyear Budgets

The PM-ISE is currently developing a framework with which to evaluate ISE-related investments. This framework will be consistent with OMB's principles of program management, and will incorporate a disciplined process to ensure that procurement of and investments in systems and technology are consistent with the ISE IP and comply with IRTPA 1016(h)(2)(D). In addition, the PM-ISE is establishing standardized, repeatable processes that support rigorous analysis of the financial and program-specific data collected.

In order for the ISE to meet the information sharing requirements set forth in the law and achieve goals stated in the ISE IP, ISE participants must invest in a common set of key capabilities and functional services. ISE organizations much share equal responsibility for identifying resources for ISE investment in a consistent and coordinated manner. The following four ISE Investment Priorities will help to advance the ISE by FY 2009: SAR (Presidential Guideline 2), the SBU/CUI Framework (Presidential Guideline 3), the ITACG/ State and Major Urban Area Fusion Centers (Presidential Guideline 2), and the ISE shared space (Presidential Guideline 1). Although these priorities will evolve throughout the life of the ISE based upon ISE mission requirements and stakeholder

needs, they will net a first set of improved, tangible, terrorism-related information sharing capabilities.

The following investment objectives will allow for informed decisions and result in increased efficiency in utilizing the resources needed to meet ISE requirements: (1) strengthen Agencies' ISE-related budget submissions by increasing opportunities to reach a common understanding regarding the PM-ISE's expectations and resource considerations; (2) integrate program review activities to performance management initiatives to monitor Agency progress toward the full implementation of the ISE; and (3) assist Agencies in developing sound investment strategies that are aligned to ISE goals. The PM-ISE is working closely with OMB to ensure a system is in place to achieve the desired outcomes.

To accomplish the first objective, the PM-ISE, in coordination with OMB, will assist Agencies in gathering information regarding ISE-related capability requirements and cost data. Using this information, the PM-ISE will develop cost methodologies to establish a baseline that will be the foundation for future FY expenditures, thereby creating the capabilities to determine and report "what was spent in the preceding year," as required by IRTPA Section 1016(h)(2)(C) and (D). The PM-ISE will accomplish the second objective by establishing appropriate performance measures, with associated targets, that are consistent with the three performance management perspectives discussed in Section 6.0 of this Report. In addition, and in coordination with OMB, the PM-ISE will evaluate and monitor the execution of funds for ISE components to assess if additional funding is required to produce the necessary results.

In keeping with the third objective of strengthening Agencies' ISE-related budget submissions, the PM-ISE, in coordination with OMB, has developed Budget Guidance to assist ISC Member Agencies in identifying FY2009 funding requests for investments that support a select number of ISE-related implementation priorities.[36] The guidance was issued in the fourth quarter of FY2007, and will be used as a template for future guidance documents.

7.3 An Accounting of How Much Was Spent on the ISE in the Preceding Year

As noted above, the PM-ISE used the 2006 Program Reviews to better understand the Federal programs, systems, and activities that were considered key to the foundation of the ISE. Therefore, one of the objectives of the 2007 Program Reviews is to capture an estimate of the expenditures, or budget execution dollars. In addition, along with projected FY2009 through FY2013 expenditures, the investment framework will underscore the specific ISE initiatives to establish associated "baseline" costs for those ISE programs, systems, and activities that are aligned with ISE-related implementation

[36] The results of the process will be incorporated into the OMB "passback" process.

priorities. Future changes in FY expenditures can then be determined in out years, and reported in subsequent ISE annual reports.

Appendix 1 – Acronyms

ADNI/CIO	Associate DNI/Chief Information Officer
C&A	Certification and Accreditation
CC	Coordinating Committee
CDS	Cross Domain Solution
CI/KR	Critical Infrastructure and Key Resource
CIA	Central Intelligence Agency
CICC	Criminal Intelligence Coordinating Council
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
CLASS	Consular Lookout and Support System
CNSS	Committee on National Security Systems
CTISS	Common Terrorism-related information Sharing Standards
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DoD	Department of Defense
DOE	Department of Energy
DOI	Department of the Interior
DOJ	Department of Justice
DNI	Director of National Intelligence
E.O.	Executive Order
EAF	Enterprise Architecture Framework
EDS	Electronic Directory Service
EU	European Union
FBI	Federal Bureau of Investigation
FCCG	Fusion Center Coordination Group
FGISWG	Foreign Government Information Sharing Working Group
FY	Fiscal Year
GCC	Government Coordinating Councils
GLOBAL	Global Justice Information Sharing Advisory Group
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
IA	Information Assurance
IACP	International Association of Chiefs of Police
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council
ISE	Information Sharing Environment

ISE IP	Information Sharing Environment Implementation Plan
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
MOA	Memorandum of Agreement
MPPIP	Model Privacy Policy Implementation Process
NCIC	National Crime Information Center
NCTC	National Counterterrorism Center
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NOL	National Counterterrorism Center (NCTC) Online
NSA	National Security Agency
NSC	National Security Council
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCII	Protected Critical Infrastructure Information
PGC	Privacy Guidelines Committee
PM-ISE	Program Manager for the Information Sharing Environment
SAR	Suspicious Activity Reporting
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Councils
SCI	Sensitive Compartmented Information
SLIAG	Presidential Guideline 2 Senior Level Interagency Advisory Group
SLT	State/local/tribal
State	Department of State
TECS	Treasury Enforcement Communications System
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
UCDMO	Unified Cross Domain Management Office