OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Information Sharing Environment 2017 Annual Report to Congress

LEADING INTELLIGENCE INTEGRATION

TABLE OF CONTENTS

BACKGROUND – LEGISLATIVE REQUIREMENT

Section 1016 of the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)* requires the establishment of an Information Sharing Environment (ISE), "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."

This report is submitted in accordance with section 1016(h) of the IRTPA which specifies that the annual report to the Congress address the following:

Table 1. IRTPA Annual Reporting Requirements

Summary of Progress:	The extent to which the ISE has been implemented, including how the ISE has fared on the performance measures and whether the performance goals set in the preceding year have been met.
Performance Objectives:	Objective system-wide performance goals for the following year.
Cost and Accounting/ ISE Investments:	How much was spent on the ISE in the preceding year.
	Actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE.
Watch Lists and Screening:	The extent to which all terrorism watch lists are available for combined searching 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.
State, Tribal, and Local Partner Participation:	The extent to which state, local, and tribal officials are participating in the ISE.
Private Sector Participation:	The extent to which private sector data, including information from owners and operators of critical infrastructure, are incorporated in the ISE.
Information Accuracy:	The measures taken by the Federal Government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals.
Privacy and Civil Liberties Protections:	An assessment of the privacy and civil liberties protections of the ISE.
Information Security:	An assessment of the security protections used in the ISE.

SUMMARY OF PROGRESS

Over the past year, federal departments and agencies have continued to make significant progress to strengthen the sharing of terrorism-related information among federal, state, local, tribal, and private sector (FSLT/PS) partners.

As noted by the Government Accountability Office (GAO) in their February 2017 report to the Congress, federal departments and agencies have successfully executed an ISE implementation plan and have demonstrated that various information sharing initiatives are being used across multiple agencies as well as FSLTT/PS stakeholders.[1]

In a recent report by the Inspectors General (IG) from the Intelligence Community (IC), Department of Homeland Security (DHS), and the Department of Justice (DOJ) to the Senate Select Committee on Intelligence, the Senate Homeland Security and Governmental Affairs Committee, and the Senate Judiciary Committee, the Inspectors General indicated that FSLTT/PS partners in the information sharing environment are committed to sharing Counterterrorism (CT) information. The report further indicated that the partners' commitment to protecting the nation is illustrated by the actions taken before, during, and following terrorism-related incidents, as well as by programs and initiatives designed to improve sharing of CT information.[2]

While the progress described in these reports is noteworthy, the GAO noted that the Federal Government has yet to eliminate all risks associated with terrorism-related information sharing.[3] Both reports highlight the need for departments and agencies to continue their efforts to advance and sustain the ISE.

The protection of privacy, civil rights, and civil liberties (P/CRCL), mandated by both the Privacy Act and the IRTPA, as well as Executive Order 12333, is a core tenet of the ISE, and remains a priority. ISE mission partners remain cognizant of—and continue to improve—safeguards to ensure the protection of the P/CRCL of citizens.

Federal ISE partners continue to prioritize safeguarding information, largely through policies, procedures, and technology focused on countering insider threat, identity authentication, reducing anonymity, controlling access to data, and information technology (IT) enterprise audits.

---

[1] GAO-17-317, February 2017, Establishing Effective Mechanisms for Sharing and Managing Terrorism-Related Information to Protect the Homeland, p. 653.

[2] Review of Domestic Sharing of Counterterrorism Information, March 2017, Prepared by the Inspectors General of the: Intelligence Community, Department of Homeland Security, and Department of Justice, p. i.

[3] GAO-17-317, p. 653

PERFORMANCE OBJECTIVES

The President's 2012 National Strategy for Information Sharing and Safeguarding (NSISS) continues to provide the focus for federal departments' and agencies' information sharing efforts. These efforts, which are derived from the NSISS, are centered on the five strategic information sharing and safeguarding goals:

- Drive Collective Action through Collaboration and Accountability;
- Improve Information Discovery and Access through Common Standards;
- Optimize Mission Effectiveness through Shared Services and Interoperability;
- Strengthen Information Safeguarding through Structural Reform, Policy, and Technical Solutions; and
- Protect Privacy, Civil Rights, and Civil Liberties through Consistency and Compliance.

Within the IC information environment, information sharing performance is further focused on these goals and objectives:

- Enhance Intelligence Integration;
- Optimize Information Assurance to Secure and Safeguard the IC Enterprise; and
- Operate as an Efficient, Effective IC Enterprise.

While terrorism-related information sharing among key federal departments and agencies has improved, according to GAO reporting and the IG findings and recommendations, terrorism related information sharing across the Sensitive but Unclassified (SBU) fabric among ISE partners remains an area where additional improvements are needed.[4] ISE objectives designed to improve SBU information sharing include:

- Enhance interoperability between ISE partners on the SBU fabric;
- Validate SBU objective architecture, standard operating procedures, policies, and protocols for ISE partners;
- Expand SBU information access through common agreements, standard protocols, and information technology advancements;
- Ensure availability of common SBU applications for ISE partners; and
- Migrate shared services to a common space (e.g., an SBU cloud).

[4] GAO-17-317, p. 658.

COST AND ACCOUNTING OF ISE INVESTMENTS

Federal Department and Agency ISE Investments

ISE-related investments are included in agency information technology investment portfolios which are reported via the Office of Management and Budget's (OMB) annual Information Technology (IT) portfolio data request.[5] Each agencies' budget year IT investments are displayed on OMB's IT Dashboard - https://myit-2017.itdashboard.gov/

Incremental costs related to implementing the ISE are embedded within each department's mission activities and operations and are not reported separately within each department's IT portfolio. For this reason, since 2013, there has been no attempt to delineate ISE related investments from department and agency IT investments in the Annual ISE Report to Congress.

Further, the Government Accountability Office (GAO) recognized that department and agency ISE investments are part of their overall IT investment portfolios, as noted here:

> *"In our 2011 report (GAO-11-455) on the Environment, we recommended that key departments better define incremental costs for information sharing activities, so as to plan and budget for these costs. ... In 2014, officials from each of the five key departments said that information sharing activities are a daily activity that go hand in hand with the mission of the agency and related budgets, and are not separate mandates to fund. Therefore, there is no need to separately identify incremental costs since information sharing activities and costs are embedded within the agency's mission operations. "* [6]

ISE Management Efficiencies

In June 2016, the office of the Program Manager for the Information Sharing Environment (PM-ISE) was placed under the leadership of the Assistant Director of National Intelligence for Partner Engagement (ADNI-PE). The action was a result of internal Office of the Director of National Intelligence (ODNI) reviews by Systems & Resource Analyses, Policy & Strategy, and the IC IG.

The merger of ADNI-PE and PM-ISE has resulted in increased effectiveness for both organizations. ADNI-PE is working to streamline operations, such as human resources, personnel hiring actions, resource management, contract oversight, and administrative support, to improve business processes and realize costs savings from combined operations.

Separately, the 21% reduction in the PM-ISE budget from FY16 to FY17 drove greater efficiencies and synchronization of legacy PM-ISE activities and ODNI offices, such as the National Counterterrorism Center (NCTC), the IC Chief Information Officer, and the National

---

[5] Executive Office of the President, Office of Management and Budget Circular A-11 Preparation, Submission, and Execution of the Budget, Exhibit 53 Agency Information Technology Investments

[6] GAO-15-290 High Risk Series, February 2015, p. 223

Intelligence Manager for Western Hemisphere and Homeland. These enhanced intra-ODNI partnerships have helped advance broader IC information sharing and safeguarding mission objectives.

WATCH LISTS AND SCREENING

The Terrorist Screening Center (TSC) is administered by the Federal Bureau of Investigation (FBI) with support from DHS, Department of State (State), DOJ, Department of Defense (DoD), the Department of the Treasury, and the Office of the Director of National Intelligence (ODNI), and is the U.S. Government's consolidated CT watch listing component responsible for the management and operation of the Terrorist Screening Database (TSDB), commonly referred to as the "terrorist watch list." NCTC's Terrorist Datamart Environment (TIDE) is the U.S. Government's central classified repository of all known or suspected international terrorists and their networks, and populates the TSDB with unclassified subsets of this data.

The TSDB contains sensitive national security and law enforcement information concerning the identities of those who are known or reasonably suspected of being involved in terrorist activities. The TSC ensures the timely dissemination of terrorist identity information from the TSDB to its screening partners, including FSLTT law enforcement, to create a well-informed terrorist screening network critical to the U.S. Government's efforts to detect and interdict known or suspected terrorist activities.

NCTC is a key partner in the screening and vetting enterprise, screening all visa, visa waivers, refugee-asylum, and other immigrant benefit applicants against data in TIDE. The results are shared with DHS and State for benefit adjudication.

In 2016, the watch listing and screening enterprise fully implemented the Watch Listing Guidance (WLG) which was published in December 2015. The interagency developed and coordinated the updated WLG, which included a modification to the definition of *NO FLY* and which takes into account the phenomenon of homegrown violent extremists. The result of the action provided greater operational flexibility to watch listing and screening partners.

The TSC also provides a subset of the watch list to its foreign partners. In 2016, the TSC made substantial gains in its partnerships with foreign entities, increasing the number of foreign partners to over 50.

In 2016, DHS, which manages the Traveler Redress Inquiry Program (TRIP), fully implemented new protocols for managing *NO FLY* inquiries made by U.S. persons. Through TRIP, individuals who believe they are incorrectly on the watch list can ask that their records be reviewed. In the case of a *NO FLY* inquiry, the subject is now permitted to review the unclassified or declassified derogatory information which led to the watch listing decision.

STATE, TRIBAL, AND LOCAL PARTNER PARTICIPATION

While progress has been made with state, local, and tribal participation in the ISE, more work is needed to continue advancing the use of interoperable systems, shared services, federated searches, and access management.

Federal ISE partners, to include DHS and FBI, work closely with the National Network of Fusion Centers to integrate state, local, tribal, and territorial (SLTT) entities into the ISE. The Fusion Centers, which operate as state and major urban area focal points for the receipt, analysis gathering, and sharing of threat-related information among ISE partners, bring critical context and value to homeland security and law enforcement.

In 2016, DHS enhanced the Fusion Centers' capabilities by deploying the Request for Information Exchange (RFI Exchange) application to the Homeland Security Information Network (HSIN). RFI Exchange provides Fusion Centers with the ability to request and share information among other Fusion Centers and with the TSC. In 2016, all 78 independent Fusion Centers across the U.S. and its territories collaborate and share requests for information.

Additionally, DHS conducted an annual Fusion Center assessment to determine the impact of the National Network on information sharing to protect the homeland and to guide SLTT partners' information sharing priorities. The 2016 Fusion Center assessment concluded that the National Network reached its full operational capability and recommends focusing on specific impact to protect the homeland. The assessment further concluded the need to develop performance measures that will help individual Fusion Centers highlight successes and identify needed growth areas.

In 2016, the federal partners responsible for information sharing strengthened their relationship with the Criminal Intelligence Coordinating Council (CICC). The CICC is made up of members representing law enforcement and homeland security agencies from all levels of government and supports SLTT law enforcement and homeland security agencies to develop and share criminal intelligence and information nationwide. The CICC also collaborates with federal partners—including DOJ, DHS, FBI, and ODNI—to coordinate national initiatives focused on intelligence and information sharing.

The DHS Office for Community Partnerships (OCP) directly engages with SLTT partners to raise awareness of trends and patterns of ideologically-motivated violence across U.S. communities. DHS Counter Violent Extremism (CVE) information sharing planning includes CVE training resources for state, tribal, and local partners and emphasizes the role of Fusion Centers and the nationwide Suspicious Activity Report (SAR) Initiative.

The Interagency CVE Task Force is hosted by OCP, providing a mechanism for interagency cooperation and information sharing on domestic CVE, including state and local law

enforcement partners. In an effort to improve engagements and information sharing at the state and local level, OCP partnered with the Office of the ADNI-PE on a pilot project to support CVE prevention and intervention activities in Denver, Colorado. The project supports the DHS OCP Field Coordinator in Denver and the CVE activities of the U.S. Attorney.

The Joint Counterterrorism Assessment Team (JCAT) is a National Counterterrorism Center (NCTC)-led group of intelligence, law enforcement, fire service, public health, and intelligence officers that facilitates increased information sharing among IC and FSLTT/PS partners. JCAT was established by NCTC, DHS, and FBI in 2013, and was preceded by the Interagency Threat Assessment and Coordination Group (ITACG). The ITACG, established in 2007 under the Implementing Recommendations of the 9/11 Commission Act, furthered the progress toward information sharing between the IC and SLTT partners.

JCAT's mission is to improve information sharing and enhance public safety. In coordination with the FBI and DHS, JCAT collaborates with other members of the IC to research, produce, and disseminate CT intelligence products for FSLTT agencies and the private sector.

JCAT analysts continue work regularly with IC partners to produce and disseminate CT intelligence products through already established dissemination mechanisms at the lowest classification level for SLTT/PS first responders. JCAT members are situated within NCTC, allowing federal analysts and SLTT partners to review classified draft products and provide a SLTT's perspective. This allows JCAT to advocate for SLTT equities during the analytic production process and thereby enables the production of analytic products, guides, and handbooks at lower classification levels.

Organizationally, the JCAT Director is appointed by the Director of NCTC, and supported by two senior-level deputies from DHS and FBI. NCTC, DHS, and FBI each contribute federal intelligence analysts and sponsor SLTT first responders as executive fellows.

PRIVATE SECTOR PARTICIPATION

Private sector participation in the information sharing environment continues to mature as existing organizations and information sharing protocols within ODNI, DHS, and FBI develop and mature.

The Domestic Security Alliance Council (DSAC), led by the FBI, is a strategic partnership between the U.S. government and U.S. private industry to enhance information sharing and the timely and effective exchange of security and intelligence information between the federal government and the private sector. The DSAC promotes efforts to advance the FBI's mission of detecting, preventing, and deterring criminal acts by facilitating strong, enduring relationships among its private sector member companies, FBI Headquarters, FBI field offices, DHS Headquarters and Fusion Centers, and other federal government entities.

DHS's National Protection and Programs Directorate (NPPD) shares responsibility for coordinating private sector participation in the information sharing environment. Specifically NPPD is responsible for the protection of the Nation's physical and cyber critical infrastructure from terrorist attacks, natural disasters, and other catastrophic incidents. NPPD also works with private sector partners to integrate both government and private sector information into the ISE.

INFORMATION ACCURACY

The measures taken by the watch listing enterprise to ensure the accuracy of terrorism related information in the ISE are outlined in the WLG adopted in December 2015. The WLG lays out a standard framework, with minimum derogatory standards, and minimum identifying criteria, to ensure the watch listing community has a standard to determine an individual's eligibility for presence on the watch list. WLG also provides the specific criteria needed to ensure proper identification during screening.

The 2015 WLG, as in previous versions, requires nominating agencies to establish and maintain quality control processes and training to ensure that the information transmitted to NCTC is accurate. Agencies also have a continuing responsibility to notify NCTC of any changes that affect accuracy, validity, or reliability of information they have previously provided. NCTC reviews TIDE records for quality assurance purposes, and coordinates with TSC on the removal of subjects from TIDE or the watch list based on, for example, a determination that the subject has no association with terrorism; the accuracy, credibility, or reliability of the information; the availability of unique identifying data; or the existence of mitigating factors or extenuating circumstances.

DHS has separate processes in place to continually ensure information accuracy. For example, Customs and Border Protection (CBP) utilizes matching algorithms to compare identities from TECS (not an acronym) records against identities in the TSDB. When a potential match is identified, NCTC will adjudicate the match and pull information from CBP holdings that can augment or enhance the data contained in the TSDB record. Transportation Security Administration (TSA) also contributes information derived from encounters with known or suspected terrrorists (KSTs) directly into TIDE via the DHS watch list framework. After the information is entered into TIDE, information is sent to the TSDB for vetting and screening purposes.

Additionally, the United States Citizenship and Immigration Services (USCIS) Fraud Detection and National Security Directive maintains a certified cadre of watch list analysts within DHS. These analysts are able to update biographic information from USCIS data systems into the TIDE records of KSTs or nominate appropriate family members of a KST.

Separately, in the Pre-Adjudicated Threat Recognition Intelligence Operations Team (PATRIOT) process, Immigration and Customs Enforcement Special Agents conduct in-country

interviews, as part of the visa application screening process, to aid in identity resolution, record information to enhance records, and identify information for Intelligence Information Reports (IIRs). The information contained in the IIRs is reviewed for the purpose of nominating subjects to TIDE or recommending further investigation. Additionally, visa applications are reviewed, verified through an interview process, and then vetted against DHS data holdings. Visa applications are assessed a second time once State verifies the application data, and thereafter recurrently vetted after the visa is issued.

PRIVACY AND CIVIL LIBERTIES PROTECTIONS

As previously stated, the protection of privacy, civil rights, and civil liberties (P/CRCL) is a core tenet, foundational element, and enabler of the ISE. In 2005, the Administration called for the development of a protection framework, resulting in the development of ISE Privacy Guidelines to provide uniform protections for P/CRCL in information sharing activities.

The ISE Privacy Guidelines establish a P/CRCL protection framework, which requires both federal and non-federal entities seeking to access "Protected Information" in the ISE to:

- develop and adopt written privacy policies,
- designate a privacy and civil liberties officer,
- provide training to ISE personnel on P/CRCL protections, and
- integrate the P/CRCL protections and requirements into business processes and systems.

Internal to the IC, ODNI's Civil Liberties, Privacy, and Transparency (CLPT) office is actively engaged with stakeholders in implementing the requirements mandated by Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and the National Insider Threat Policy and Minimum Standards for executive branch insider threat programs, including developing an ODNI insider threat program that is consistent with an individual's P/CRCL protections.

As needed, CLPT provides support to the National Insider Threat Task Force (NITTF), as it continues to assess and assist executive branch insider threat programs in becoming fully operational and leads a Government-wide effort to improve insider threat program capabilities.

CLPT continues to perform its advisory and compliance role with respect to the activities of the NCTC, the component within the ODNI primarily responsible for CT intelligence analysis and CT strategic operational planning.[7] CLPT provided guidance regarding conditions for NCTC's receipt, use, retention, and dissemination of data and worked closely with NCTC to develop

[7] Additional information about NCTC is available at www.dni.gov.

policies for access, use and tracking of certain categories of data containing personally identifiable information.

CLPT worked to ensure that its web-based course on the Privacy Act and protections for personally identifiable information became designated as mandatory for ODNI personnel, contractors, detailees, and assignees. This training serves as a required follow-up to the overview privacy training provided to all employees at their entry on duty (EOD) orientation. New employees must take this required web-based course within 30 days of EOD and all personnel annually thereafter.

DHS conducted quarterly P/CRCL reviews of CBP and TSA's real-time, threat-based intelligence scenarios run by the Automated Targeting System (ATS) to ensure that P/CRCL protections were in place. ATS is a decision-support tool used by CBP to improve the collection, use, analysis, and dissemination of information collected to target, identify, and prevent terrorists from entering the United States.

Additional DHS P/CRCL activities and initiatives include:

- a Privacy Compliance Review of DHS's participation in the Nationwide SAR Initiative;
- collaboration on the development and deployment of technologies that may impact civil rights and civil liberties to build in appropriate safeguards designed to protect civil rights and civil liberties;
- bi-monthly reviews of technologies for countering unmanned aerial systems and nontraditional aviation technology, and the use of legal authorities for countering these systems, for civil rights and civil liberties equities; and
- the review of agency policies relating to the use of body cameras in support of law enforcement operations.

INFORMATION SECURITY

A key information security issue is how ISE partners might deter, detect, and mitigate compromises of information by malicious insiders. Established after the 2010 WikiLeaks release of classified documents, the NITTF's primary mission, pursuant to EO 13587 and the National Insider Threat Policy, is to develop a U.S. Government-wide insider threat program for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies.

The NITTF is co-chaired by the Attorney General and the DNI, and is currently directed by a senior executive from the National Counterintelligence and Security Center. The task force's work impacts approximately 100 federal departments and agencies that handle or access

classified information. In light of this broad mission scope, the task force has drawn together expertise from across the government in the areas of security, counterintelligence, information assurance and others to develop the policies, standards, guidance and training necessary for individual departments and agencies to implement insider threat programs. Part of the NITTF effort involves providing departments and agencies with assistance to better educate their workforce to recognize potential insider threat activity without creating an atmosphere of distrust.

Presidentially mandated *Minimum Standards of the National Insider Threat Program* require insider threat programs to be developed and operated in coordination with a department's or agency's records management office, legal counsel, and civil liberties and privacy officials to build in protections against improperly infringing upon employees' P/CRCL or whistleblower protections. Departments and agencies are required to provide training in these areas to insider threat program personnel, as well as to the general workforce. Department and agency heads also have a responsibility to ensure these protections are maintained through oversight of their insider threat programs.

Insider threat programs look for anomalous activities. They do not target individuals. Government employees who handle classified information understand that, to hold a security clearance, they accept additional oversight of their workplace activities. Employees sign authorizations for the conduct of investigations to obtain and retain security clearances, and there are warning banners on computers and in certain areas of facilities that alert people that they have less expectation of privacy.

In May 2014, the National Security Council's Deputies Committee, in an effort to drive progress in implementing the Minimum Standards, set December 31, 2016 as the goal for all executive branch departments and agencies to have a fully operational insider threat program. Based on NITTF independent assessments, the executive branch made slow, but steady progress towards meeting the goal; however, not all executive branch departments and agencies were able to meet the December 31, 2016 goal. NITTF assessments have identified several significant challenges that persist: a lack of adequate resources to conduct insider threat program operations; inconsistent legal interpretations of program requirements and agency authorities; and technical and policy constraints of monitoring user activity on classified networks. These challenges hindered many departments' and agencies' ability to achieve fully operational, insider threat programs. NITTF continues to work with the insider threat community to meet these challenges.

A key focus area for the NITTF in 2017 is the development of a framework to improve the effectiveness of insider threat programs. While the Minimum Standards created the necessary building blocks for insider threat programs, there is currently no construct to ensure insider threat programs are operating effectively across the executive branch. The NITTF, in coordination with the insider threat community, is developing this framework to advance insider threat deterrence, detection and mitigation capabilities.

ABBREVIATIONS AND ACRONYMS

ATS	Automated Targeting System
CBP	Customs and Border Protection
CICC	Criminal Intelligence Coordinating Council
CLPT	Civil Liberties, Privacy, and Transparency
CT	Counterterrorism
CVE	Counter Violent Extremism
DHS	Department of Homeland Security
DoD	Department of Defense
DOJ	Department of Justice
DSAC	Domestic Security Alliance Council
EOD	Entry on Duty
FBI	Federal Bureau of Investigation
FSLT/PS	Federal, State, Local, Tribal, and Public Sector
GAO	Government Accountability Office
HSIN	Homeland Security Information Network
IC	Intelligence Community
IIR	Intelligence Information Report
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
IT	Information Technology
ITACG	Interagency Threat Assessment and Coordination Group
JCAT	Joint Counterterrorism Assessment Team
KST	Known or Suspected Terrorist
NCTC	National Counterterrorism Center
NITTF	National Insider Threat Task Force
NPPD	National Protection and Programs Directorate
NSISS	National Strategy for Information Sharing and Safeguarding
OCP	Office of Community Partnerships

ODNI	Office of the Director of National Intelligence
PATRIOT	Pre-Adjudicated Threat Recognition Intelligence Operations Team
P/CRCL	Privacy, Civil Rights, and Civil Liberties
SAR	Suspicious Activity Report
SBU	Sensitive But Unclassified
SLTT	State, Local, Tribal, and Territorial
State	Department of State
TIDE	Terrorist Identities Datamart Environment
TRIP	Traveler Redress Inquiry Program
TSA	Transportation Security Administration
TSC	Terrorist Screening Center
TSDB	Terrorist Screening Database
USCIS	United States Citizenship and Immigration Services
WLG	Watch Listing Guidance