Office of the Director of National Intelligence

(U) 2018 Information Sharing Environment

Leading Intelligence Integration

October 2018

Contents

(U) BACKGROUND – LEGISLATIVE REQUIREMENT 3

(U) PURPOSE AND SCOPE 3

(U) SUMMARY 3

(U) PERFORMANCE OBJECTIVES 4

(U) ISE INVESTMENTS 5

(U) TERRORISM WATCHLISTING AND SCREENING 6

(U) STATE, LOCAL, AND TRIBAL PARTICIPATION IN THE ISE 11

(U) PRIVATE SECTOR PARTICIPATION IN THE ISE 15

(U) ACCURACY OF INFORMATION 16

(U) PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS 17

(U) INFORMATION SECURITY PROTECTIONS 17

(U) WAY AHEAD 19

(U) APPENDIX A - ACRONYMS 20

(U) BACKGROUND – LEGISLATIVE REQUIREMENT

(U) The Annual Report to the Congress on the Information Sharing Environment (ISE) is submitted in accordance with requirements in Section 1016(h) of *the Intelligence Reform and Terrorism Prevention Act of 2004*, as amended (IRTPA) and serves as "a progress report on the extent to which the ISE has been implemented."[1]

(U) PURPOSE AND SCOPE

(U) This report highlights continued enhancements to the ISE by selected federal, state, local, tribal (FSLT), and private sector partners. Information in this report not only illustrates the value of the ISE in sharing terrorism related information, as intended by the IRTPA, but also how the policies, procedures, technologies, and agreements that have matured with the ISE can be applied to other national security related threats.

(U) SUMMARY

(U) In the past year, continued progress has been accomplished across the ISE in achieving goals and objectives to improve interoperability and expand information access among FSLT, and private sector partners.

(U) Within watchlisting and screening processes, significant improvements were achieved, particularly with the establishment of updated minimum screening data standards for travelers or certain benefit applicants and the implementation of the concept of a "consolidated initial check." Additionally, the United States Government (USG) continues to expand information sharing with foreign partners, to include sharing data on criminal history, known or suspected terrorists (KST), and foreign fighters, either through existing or new bilateral information sharing arrangements.

(U) Information sharing partnerships among the Federal Bureau of Investigation (FBI) field offices, deployed Department of Homeland Security (DHS) personnel, fusion centers, and other field-based partners improved through the implementation of the regional integration and coordination plans and information technology improvements which support enhanced engagement for analysis and operations.

(U) Information sharing networks such as the FBI's National Data Exchange (N-DEx) System and Regional Information Sharing Systems (RISS) centers continue to enable collaboration among federal, state, and local partners. DHS's Homeland Security Information Network's (HSIN) partnerships with the Terrorist Screening Center (TSC) and the National Network of Fusion Centers

[1] IRTPA, §1016(b) (1) (A). The scope of the ISE was originally limited to "terrorism information" as defined in §1016. In August 2007, The *Implementing Recommendations of the 9/11 Commission Act of 2007* (P.L. 110-53), included amendments to §1016 that expanded the scope of the ISE to explicitly include homeland security and weapons of mass destruction information.

(National Network) have resulted in increased information access through HSIN Exchange. Additionally, a nationwide communications infrastructure, built specifically for the Nation's first responder community – FirstNet – was launched providing dedicated communications.

(U) The protection of privacy, civil rights, and civil liberties remains a priority across the ISE. The Office of the Director of National Intelligence (ODNI) published in 2018 an Intelligence Community Directive (ICD 107) that provides for the oversight and guidance to the Intelligence Community (IC) on privacy, civil liberties, and transparency with respect to intelligence activities conducted by IC elements.

(U) Finally, the attributes of the ISE were recognized as valuable to meet the information sharing needs associated with other national security related threats. For example, the Government Accountability Office (GAO),[2] described the importance of information sharing between FSLT law enforcement and the private sector as key to countering the distribution and use of illicit opioids. Officials have realized the ISE related information sharing policies, procedures, technologies, and agreements can be leveraged to mitigate other national security related threats.

(U) PERFORMANCE OBJECTIVES

(U) The goals in the 2012 National Strategy for Information Sharing and Safeguarding (NSISS) continue to provide the focus for federal departments' and agencies' information sharing efforts:

- 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.

(U) Within the IC, the 2016-2020 Information Technology Enterprise Strategy and the 2017-2021 IC Information Environment Data Strategy together provide additional implementation guidance:

- enhance intelligence integration;
- optimize information assurance to secure and safeguard the IC enterprise;
- operate as an efficient, effective IC enterprise;
- develop and institutionalize a strategic data framework across the multi-fabric IC information environment;
- ensure data is appropriately protected, shared, and handled across all fabrics;

[2] GAO-18-205 Combating Synthetic Opioids, March 2018

- create, resource, and leverage secured, scalable and shared data services that meet the IC's needs for variety, velocity, volume, and veracity; and
- champion a culture that encourages and rewards data-centric behaviors that effectively balance sharing and safeguarding.

(U) ISE objectives designed to improve Sensitive but Unclassified (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).

(U) ISE INVESTMENTS

(U) As reported in 2017, ISE-related investments are included in agency information technology (IT) investment portfolios which are reported via the Office of Management and Budget's (OMB) annual IT portfolio data request.[3] Each agency's budget year IT investments are displayed on OMB's IT Dashboard - https://myit-2017.itdashboard.gov. For this reason, since 2013, there has been no attempt to delineate ISE specific investments within department and agency IT investments. In 2015, the GAO further recognized that federal department and agency ISE investments inherently are part of their overall IT investment portfolios, as noted here:

> ***"... 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. "*** [4]

(U) ISE Initiatives Program

(U) The Program Manager Information Sharing Environment (PM-ISE), through the Information Sharing Council (ISC), annually solicits proposals for information sharing projects that enable responsible information sharing across the ISE and expand collaboration efforts with federal, state, local, and tribal partners while preserving civil liberties and privacy.

[3] 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

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

(U) The ISE Initiatives Program (IIP) allows the PM-ISE to prioritize partner requirements, optimize SBU[5] information sharing with state and local partners, and implement information sharing and safeguarding solutions to protect the homeland. Since 2015, the PM-ISE has provided project funds enabling a wide range of federal, state, and local information sharing projects.

(U) In the coming year, PM-ISE is prioritizing projects that: further improve terrorism-related information discovery and access; optimize interoperability; enable improved accuracy of information about individuals; and further advance information sharing among federal, state, and local partners using existing systems. All of these efforts align with IRTPA information sharing attributes, and support both the 2012 National Strategy for Information Sharing and Safeguarding and the current National Security Strategy.

(U) TERRORISM WATCHLISTING AND SCREENING

(U) National Counterterrorism Center

(U) The National Counterterrorism Center (NCTC) has continued to play a critical role in the ISE by responsibly and securely sharing classified terrorism information with screening partners and adjudicators. In response to Executive Order (EO) 13780[6], NCTC, in cooperation with its screening partners, expanded the scope of counterterrorism (CT) screening in 2018 to access a broader range of derogatory information.

(U//~~FOUO~~) NCTC visa application assessments are shared with screening partners and include relevant biometric data, biographic information, and any derogatory information. These data sets are incorporated into Terrorist Identity Datamart Environment (TIDE), while the biometric data and biographic information are subsequently sent to TSC for enhancing records in the Terrorist Screening Database (TSDB). The TSC makes the appropriate screening information available to FSLT and international partners, including front line screeners, to share identity intelligence information and constrain global terrorist travel.

(U) In June 2017, NCTC and Customs and Border Protection (CBP) launched an improved screening system resulting in the automation of CT checks for travelers from visa waiver countries, who are eligible to use the Electronic System for Travel Authorization (ESTA) to apply for travel to the U.S. The screening change provides CBP near real time TIDE CT checks. Through NCTC's Kingfisher Expansion ESTA (KFE-E) platform, ESTA applications are screened against TIDE before the ESTA

[5] Executive Order 13556, *"Controlled Unclassified Information"* (CUI), November 4, 2010, standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. State and local partners refer to CUI as Sensitive but Unclassified (SBU).

[6] EO 13780 *"Protecting the Nation from Foreign Terrorist Entry into the United States",* March 9, 2017, requires the Executive Branch to implement uniform screening and vetting standards in connection with immigration programs, including the visa adjudication process and the United States Refugee Admissions Program (USRAP).

approvals are issued. This aligns ESTA with the other visa and immigrant benefit screening processes. Prior to the KFE-E launch, some of the individuals who were able to travel to the U.S. before the TIDE check were later identified as having connection to terrorism. The upgraded program closes this national security risk and supports NCTC's review of more than 14 million ESTA requests annually.

(U//~~FOUO~~) NCTC continues to exercise consistent standards in reviewing TIDE records for quality assurance purposes, and coordinates with TSC on the removal of subjects from TIDE or the watchlist. Such removals are 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.

(U) Other important enhancements to the watchlisting and screening enterprise include the establishment of minimum screening data standards for personal information submitted by travelers or benefit applicants, and the implementation of a "consolidated initial check." The minimum required personal information reflects the type of high-value data that creates a clear biographic data-representation or picture of the individual, which will enable greater automated matching to terrorism-related threat information, while minimizing false positive matches. The clearer data-picture will increase the accuracy of the information on individuals, reduces identification errors, and facilitates legitimate travel and benefit authorizations.

(U) Terrorist Screening Center

(U//~~FOUO~~) In addition to providing watchlisting information to TSC's FSLT partners, the TSC manages and maintains the USG's terrorism screening information sharing arrangements with international partners. Under Homeland Security Presidential Directive 6 (HSPD-6)[7], the TSC shares USG terrorism-related biographic and encounter information, including the identities of high-risk foreign terrorist fighters (FTFs), with our international partners to facilitate screening, vetting, law enforcement investigations, and intelligence sharing.

(U//~~FOUO~~) In the past year, the TSC, in cooperation with the Department of State, made substantial gains in the number of its partnerships with international entities, thereby increasing the number of international partners receiving and utilizing a subset of the TSDB to over 70; 12 of those partnership agreements were signed or implemented in 2017. In addition, the TSC is engaged in discussions with more than 20 potential partner nations regarding future HSPD-6 relationships. Over the past year, more than half of the TSC's partner nations have shown an increase in sharing; either through their submissions of KST identities, or through reporting of encounters with terrorism-related identities provided by the TSC.

(U//~~FOUO~~) TSC is committed to strengthening international information sharing arrangements. In 2018, the TSC sent delegations to seven partner nations to provide additional training and technical

[7] Homeland Security Presidential Directive/HSPD–6, "Directive on Integration and Use of Screening Information To Protect Against Terrorism", *September 16, 2003*

support in an effort to improve the sharing of international biographic and encounter information. These sustainment missions have contributed to the over 140% increase in identities reported by international partners in the past year. By strengthening the capabilities of our foreign partners, the TSC expands the reach of the U.S. watchlisting enterprise and improves its ability to monitor global terrorist travel.

(U/~~FOUO)~~ Additionally, the TSC recently entered into an arrangement with International Criminal Police Organization (INTERPOL) Washington, U.S. National Central Bureau (USNCB), DOJ, by which FTF information is provided to the USNCB and then disseminated to specific international partners via the INTERPOL's network. This arrangement and a similar agreement with EUROPOL, allow an expanded screening capability against TSDB holdings. Another arrangement with the USNCB facilitates a pilot project to transfer information on stolen or lost travel documents via INTERPOL, a key element in securing U.S. borders.

(U) The U.S. Government is committed to ensuring that the watchlisting process is implemented consistent with law and is subject to numerous reviews, oversight, and provides the opportunity to seek redress, while also ensuring the information is appropriately used to vigorously protect the American public from terrorist threats, while safeguarding privacy and civil liberties.

(U) Department of State

(U/~~FOUO)~~ In 2018, the Department of State (DOS) established a Nomination Cell that centralizes all of the Department's watchlist nomination reporting for potential KST identities in the Bureau of Counterterrorism and Countering Violent Extremism (DOS/CT). DOS/CT, in coordination with Consular Affairs, Diplomatic Security, and other relevant DOS bureaus, assesses the information for accuracy, thoroughness, and reliability as a watchlist nomination. If the information meets interagency watchlisting standards, DOS/CT nominates the identity to NCTC for inclusion in TIDE and the TSDB. DOS/CT also works with its interagency partners to complete watchlisting redress and quality control requests, ensuring continued integrity of the data submitted and used by DOS.

(U) Department of Homeland Security

(U) In response to Executive Order 13780 and Presidential Proclamation 9645, DHS, in consultation with DOS, DOJ, and ODNI, developed baseline information-sharing, identity-management, and risk-factor criteria related to U.S. immigration screening and vetting against which the adequacy of foreign government cooperation is assessed on an ongoing basis. More specifically, DHS leads an interagency effort to determine whether certain and appropriate entry limitations or suspensions should be imposed, continued, terminated, modified, or supplemented, in accordance with Section 212(f) of the Immigration and Nationality Act (INA). Crucial to this effort is strategic and sustained U.S. engagement with foreign governments to encourage continued and/or improved cooperation as it relates to the baseline criteria.

(U) DHS employs a suite of information sharing tools and programs to facilitate the exchange of traveler information with foreign partners. The suite is not limited to only those tools and programs directly controlled by DHS, but also incorporates travel-related programs under the responsibility of DOS and DOJ, thereby allowing for an enhanced whole-of-government capability that partner governments may similarly undertake. The following is a representative sample of key DHS information sharing programs and activities designed to enhance the protection of the homeland.

(U) Automated Targeting System-Global (ATS-G)

(U) CBP offers the Automated Targeting System-Global (ATS) to potential foreign partner governments as a decision support tool to evaluate passengers and crewmembers prior to arrival or departure. ATS-G assists foreign government officials in the decision-making process about whether a passenger or crewmember should receive additional screening prior to entry into or departure from the country based on whether the traveler poses a potential risk for violation of the foreign country's laws and or regulations. ATS-G matches traveler data against a foreign partner's watchlist, the HSPD-6 Foreign Partner Export, INTERPOL notices, or scenario-based targeting rules.

(U) Global Travel Assessment System (GTAS)

(U) CBP developed GTAS as a secondary option for governments unwilling or unable to enter into information sharing arrangements with the U.S. CBP developed GTAS as a free, open source platform that can receive and store air traveler information enabling real-time risk-modeling. CBP donated GTAS to the World Customs Organization (WCO) in July 2017 so that it can offer GTAS to its Member Administrations at no cost and without obligation. CBP provides subject matter experts to support WCO staff in the assessment and deployment of GTAS to its members.

(U) Separately, in August 2018, DHS Science and Technology Directorate (S&T) announced it will begin testing a prototype for GTAS through a commercial award under DHS S&T's *Silicon Valley Innovation Program* (*SVIP*).[8] Developing predictive models in GTAS currently requires data scientists and specialists to work at a pace that risks obsolescence by the time a model is completed. The machine-learning prototype will test the application to GTAS of automated machine-learning to expedite model development.

(U) Biometric Identification Transnational Migration Alert Program (BITMAP)

(U) BITMAP is an Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) program in which partner-country law enforcement officers collect and share biometric and biographic data on special interest individuals to address and reduce national security, border security, and terrorist threats before such threats reach the U.S. border. BITMAP provides U.S. law enforcement and intelligence agencies targeted information on foreign partners' law enforcement encounters of persons of interest who may pose a potential threat to the U.S. or its citizens. Additionally, ICE HSI uses BITMAP to identify and map illicit pathways and emerging trends among

[8] DHS News Release: DHS Awards Virginia Company $200K to Begin Automated Machine Learning Prototype Test, August 20, 2018. https://www.dhs.gov/science-and-technology/news/2018/08/20/news-release-dhs-awards-va-company-200k-begin-automated

transnational criminal organizations; associate derogatory information with individuals; and identify known or suspected terrorists, criminals, and other persons of interest.

(U) Secure Real-Time Platform (SRTP)

(U//~~FOUO~~) SRTP is a technology platform that was originally designed to support the exchange of biometric data among Australia, Canada, New Zealand, the United Kingdom and the U.S. under Visa and Immigration Information Sharing Agreements. It is now offered to current Visa Waiver Program (VWP) countries or those countries aspiring to join VWP, and other technically capable partner countries, allowing the foreign partners to query fingerprints they collect at the border or pursuant to a criminal investigation against DHS's Office of Biometric Identity Management's (OBIM) Automated Biometric Identification System (IDENT) (including DHS, DoD, and FBI data) and allows DHS components to compare fingerprints they collect against foreign data.

(U/~~FOUO)~~ The SRTP technology allows VWP countries and aspirants to more effectively implement *Preventing and Combating Serious Crime* (PCSC) bilateral agreements. PCSC agreements provide reciprocal access to the partner's fingerprint databases for the purposes of preventing, detecting and investigating crime, including terrorism. Currently, the U.S. has 42 PCSC agreements which are managed by collaboratively by DHS and DOJ, and DOS.

(U) Biometric Data Sharing Program (BDSP)

(U//~~FOUO~~) In countries where DHS seeks the level of cooperation possible under SRTP but the partner country lacks a suitable biometric database, DHS, DOS and DoD have deployed BDSP to build partner capacity and establish interoperability between DHS and the foreign government.

(U//~~FOUO~~) Currently deployed in Mexico, through BDSP-M, the biometric data collected by the Government of Mexico's *Instituto Nacional de Migración* is made available to DHS's Automated Biometric IDENT system and compared against DHS, DoD, and DOJ data.

(U) Of note, since October 2017, DHS has received over one million queries from Australian, New Zealand, and Canadian immigration authorities; in turn, DHS compares biometric submissions for matches against select DHS component galleries.

(U) Traveler Redress Inquiry Program

(U) The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs - like airports - or crossing U.S. borders. This includes:

- watchlist issues;
- screening problems at ports of entry; and
- situations where travelers believe they have been unfairly or incorrectly delayed, denied boarding or identified for additional screening at our nation's transportation hubs.

(U) DHS TRIP is part of a U.S. Government effort to welcome legitimate travelers while still securing the Nation. DHS safeguards the privacy of any personal information provided through DHS TRIP.

(U) STATE, LOCAL, AND TRIBAL PARTICIPATION IN THE ISE

(U) Intelligence Guide for First Responders

(U) The Joint Counterterrorism Assessment Team (JCAT) is a NCTC-led group of public safety personnel and intelligence officers that facilitates increased information sharing with state and local public safety partners. JCAT products serve both domestic and international audiences. In 2017, JCAT published both Spanish-language First Responder-products, as well as English-language versions that are routinely shared with international partners. JCAT reference materials, such as the Intelligence Guide for First Responders and the CT Guide for Public Safety Personnel are unclassified and publicly available on the Internet.

(U) Enhanced Engagement Initiative

(U) The FBI, DHS, and the National Fusion Center Association (NFCA) identified a need to provide additional guidance on how the FBI can increase its engagement across the National Network to expand information and intelligence sharing and collaboration in producing timely analytic products. In coordination with NFCA and other federal partners, the FBI developed and released in Fiscal Year (FY) 18 the Enhanced Engagement Initiative (EEI) designed to provide FBI field offices and fusion centers with a common set of recommendations to ensure greater continuity and standardization of terrorism information sharing procedures.

(U) By focusing on key areas of engagement such as Joint Terrorism Task Force (JTTF) participation and coordination, suspicious activity reporting, and intelligence analysis, production, and dissemination, the EEI supports the FBI and its efforts to ensure that fusion centers have a thorough understanding of the terrorism threat, and are appropriately integrated with other field-based information sharing partners to address the ever changing threat landscape.

(U) Regional Integration and Coordination Plans

(U) In FY18, the Office of the PM-ISE, along with regional ISE partners, developed and coordinated the implementation of Regional Integration and Coordination (RIC) plans in the Northeast and Southeast regions. The RIC plans for the Western and Central regions are now under development with expected implementation later this year.[9]

(U) The RIC plans codified field-based relationships among primarily law enforcement partners and facilitates terrorism and other national security related information sharing. The plans clarify roles and responsibilities for information sharing, document coordination, and identifies interoperable

[9] The Criminal Intelligence Coordinating Council, December 2017 Meeting Highlights and Next Steps

communications systems to improve information sharing during steady-state and crisis environments. Field-based partners include fusion centers, RISS centers, High Intensity Drug Trafficking Areas (HIDTAs), and federal law enforcement partners. Specific components of a plan include:

- Investigative support;
- Intelligence analysis;
- Situational and threat awareness;
- Suspicious activity reporting;
- Requests for information (RFI);
- Information sharing and dissemination; and
- Special event support.

(U) Connecting Federal, State, Local, and Tribal ISE Partners

(U) Efforts by agencies and activities to connect existing systems to enable information sharing among agencies and between levels of government, an IRTPA attribute, continue among the ISE partners. The focus of these efforts includes connecting data holdings related to the following information sharing systems, all of which contribute to the implementation of a terrorism related ISE:

(U) National Data Exchange

(U) The N-DEx System is an unclassified criminal justice information sharing system, which ensures DOJ criminal law enforcement information is available to users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal actively, including terrorism, and protect national security. In FY17, N-DEx System usage increased significantly to more than 13 million searches, nearly doubling the activity recorded in FY16. In addition, the N-DEx Program Office continues to improve system access to FSLT partners, notably working with the RISS Program to enable N-DEx System access to RISS users.

(U) Regional Information Sharing Systems Program

(U) The RISS program, an integral part of the ISE, assists law enforcement partners by providing capabilities that facilitate information sharing, supports criminal investigations that may have a nexus to terrorism, and promotes officer safety through event deconfliction. RISS is expanding the ISE by connecting stand-alone, state and local criminal intelligence databases to the RISS Criminal Intelligence Database (RISSIntel) to more widely share criminal intelligence information.[10] In 2016 alone, RISS reported more than 10 million criminal intelligence system-to-system queries and over 350,000 views nationwide.

[10] 28 CFR Part 23 is a federal regulation that provides guidance to law enforcement agencies on the implementation standards for operating multijurisdictional criminal intelligence systems funded under the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Crime Control Act). The purpose of the regulation is to ensure the protection of constitutional (civil rights and civil liberties) rights and further an individual's reasonable expectation of privacy.

(U) Currently RISSIntel provides a real-time, online, federated search of more than 35 connected RISS and law enforcement partner criminal intelligence systems, including the Northeast region criminal intelligence data sets added in FY17. Between 2018 and 2019, RISS will add 11 additional criminal intelligence databases in the Southeast to share across the National Network, and across the RISS network. DHS Office of Intelligence Analysis (I&A) partners with the RISS Program to enable HSIN-Intel users to access RISSNET.

(U) Homeland Security Information Network

(U) In 2017, ISE partners across the FSLT and private sector landscape relied on HSIN for information sharing and collaboration. A large part of the HSIN Program's growth (2,000+ new users join every month[11]) is due to enhanced partnerships and increased operational users across all sectors. New partnerships with TSC in 2017 resulted in increased information sharing through HSIN Exchange.

(U) HSIN provides state and local officials and authorities with essential resources for use in daily operations, public safety and incident management, and supported planned and unplanned events ranging from the inauguration and high-profile sporting events, to disaster response and recovery efforts. HSIN is used in narcotics interdiction in conjunction with the HIDTA program, and relies on HSIN to support its daily operations. Law enforcement personnel now routinely use HSIN to share drug interdiction and confiscation information.[12]

(U) Homeland Security Information Network- Intelligence

(U) In 2018, the HSIN-Intelligence (HSIN-Intel) Governance Board, composed of DHS, RISS, and State/local stakeholders, planned for a multitude of technical and administrative enhancements to the HSIN-Intel portal, making the portal the primary destination for sharing unclassified products across all levels of government. Collective action by the board resulted in the implementation of major technical enhancements to HSIN-Intel's analytic collaboration capabilities, including advanced search, production planning and reporting tools, and online training. These enhancements have substantially increased support to the 4,000-plus HSIN-Intel users.

(U) HSIN Center of Best Practices

(U) In 2017, PM-ISE assisted the National Fusion Center Association in deploying a "Center of *Best Practices*" platform on HSIN-Intel that is designed to provide fusion center directors, intelligence analysts, federal partners, and other key stakeholders with easy access to program information and proven practices that have been used successfully across the national network, in support of protecting the homeland.

[11] DHS HSIN Fact Sheet, December 18, 2017

[12] Homeland Security Information Network, FY17 Annual Report, p. 15

(U) Additional benefits include an easy mechanism for sharing fusion center best practices, model policies and procedures, analytic tradecraft, as well as a suite of outreach materials to assist centers in educating public safety partners, private sectors partners, and the public.

(U) Expanding Information Sharing using HSIN

(U) In 2017, DHS expanded the Southwest Border (SWB) Intelligence and Information Sharing Community of Interest (COI) on HSIN from a SWB-focused sharing environment to one that includes all North America-based transnational organized crime (TOC) issues.

(U) The multi-agency information sharing environment, which can be accessed by federal, state, and local officials, contains finished intelligence on, among other topics, illicit financial transactions, drug trafficking, and human smuggling, all of which have documented ties to terrorism.

(U) HSIN Exchange

(U) HSIN Exchange streamlines how fusions centers manage RFIs, which are a fundamental part of fusion center daily operations.

(U) Through HSIN Exchange, analysts are able to send an RFI to a specific source, track progress, identify the person who has responded, analyze the information, and close the request. HSIN Exchange provides a secure environment that enables more efficient decision-making, removes duplication of systems and effort, and connects law enforcement and intelligence agencies to de-conflict activities.

(U) Plans for expanding the user base in 2018 include adding other partners, such as RISS centers, HIDTAs, DHS I&A, and the El Paso Intelligence Center (EPIC).[13]

(U) HSIN – Critical Infrastructure

(U) Thousands of private sector organizations rely on HSIN Critical Infrastructure (HSIN-CI) as their trusted source for SBU information to secure the nation's critical infrastructure assets. During the past year, HSIN-CI provided a more robust information sharing mechanism through an expansion of mission-focused communities of interest and enhanced content.

(U) Several new HSIN-CI communities facilitate government and industry collaboration, including Election Infrastructure Subsector, Unmanned Aircraft Systems, Chemical Medical Countermeasures, and Dams Threat Analysis Task Group, among others. In addition, the National Infrastructure Coordinating Center (NICC) provided partners with additional products and resources for risk mitigation and incident response.

(U) The Technical Resource for Incident Prevention (TRIPwire)

TRIPwire (https://tripwire.dhs.gov) is the DHS Office for Bombing Prevention's online, collaborative information and resource-sharing portal for the nation's security and emergency services professionals across the FSLT sectors to increase awareness of evolving improvised

[13] Ibid, p. 22

explosive device (IED) tactics, techniques, and procedures as well as incident lessons learned and counter-IED preparedness information.

(U) The First Responder Network Authority (FirstNet)

(U) FirstNet is the nation's first public safety community wireless broadband network that enables improved communications during emergencies and other public safety related events. Congress passed legislation to establish the network in 2012, and for the past five years, the First Responder Network Authority[14] has worked closely with the public safety community to develop customized plans for building the Network in each state and territory.

(U) As of December 2017, 50 states, five territories, and the District of Columbia have joined FirstNet. In March 2018, the First Responder Network Authority gave its private sector partner, AT&T, approval to build and deploy a public safety dedicated spectrum – Band 14 - across statewide radio networks across the country.[15]

(U) An ISC sub-committee, co-chaired by PM-ISE, consisting of representatives from within federal, state, local, and academic communities, is focused on developing FirstNet Identity Credential and Access Management (ICAM) technology and policies, to include developing ICAM acquisition guidance for state and local officials. These ICAM technologies will support FirstNet collaboration with the DHS Office of Emergency Communications.

(U) Public Safety Advisory Committee (PSAC)

(U) The 2012 Act also required FirstNet to establish a standing Public Safety Advisory Committee (PSAC) to offer FirstNet guidance and subject matter expertise and conduct outreach to the PSAC's membership—primarily comprising associations that represent different levels of government and public safety disciplines—on FirstNet's network development.

(U) PRIVATE SECTOR PARTICIPATION IN THE ISE

(U) DHS Public-Private Analytic Exchange Program

(U) The Public-Private Analytic Exchange Program (AEP), sponsored by DHS's Office of Intelligence and Analysis (DHS/I&A), on behalf of ODNI, facilitates collaborative partnerships between members of the private sector and teams of experienced U.S. government analysts to form a number of subcommittees. This annual program provides U.S. government analysts and private sector partners with a better understanding of select national security and homeland security issues.

(U) The AEP enables U.S. government analysts and private sector partners to gain a greater understanding of how their disparate, yet complementary, roles can work in tandem to ensure mission

[14] The First Responder Network Authority is an independent authority within the U.S. Department of Commerce. Chartered in 2012, its mission is to ensure the building, deployment, and operation of the nationwide, broadband network that equips first responders to save lives and protect U.S. communities.

[15] FirstNet First Responder Network Authority, Press Release, March 7, 2018

success. Participants work to create joint analytic products of interest to both the private sector and the U.S. Government. For example, past AEP efforts include identifying opportunities in applying private sector media strategies to fight terrorism. In 2018, AEP teams will focus on the following topics:

- Artificial Intelligence;
- Cyber Resilience and Response;
- Emerging Technologies and National Security; and
- Using Blockchain to store and protect data and systems.

(U) Classified Intelligence Forum

(U) The Classified Intelligence Forum is a collaborative effort between DHS/I&A and DHS National Protection and Programs Directorate (NPPD) intended to provide intelligence analysts with an opportunity to get direct feedback and insights from critical infrastructure owners and operators. This regularly-scheduled engagement brings together appropriately-cleared and identified members of the critical infrastructure community under the auspices of the Critical Infrastructure Partnership Advisory Council, providing them with access to draft or finished intelligence products.

(U) Secure Video Teleconference

(U) Secure Video Teleconferences (SVTCs) are regularly scheduled between DHS/I&A and DHS/NPPD. These engagements are designed to facilitate collaboration between fusion centers and private sector partners by providing periodic threat briefings targeting specific sectors, while also exercising processes to clear individuals to access classified space. The SVTCs are designed to provide fusion centers with an opportunity to establish and maintain relationships with private sector security representatives in their respective areas of responsibility.

(U) ACCURACY OF INFORMATION

(U) As discussed above, in the context of watchlisting and screening, special consideration and scrutiny is applied by departments and agencies associated with the watchlisting and screening processes to ensure that information about persons suspected to have a connection with terrorism is as complete, accurate, and up-to-date as possible.

(U) Further, in addition to Privacy Act[16] requirements that apply to federal departments and agencies, ISE Privacy Guidelines require each department and agency to establish data accuracy, quality, and retention procedures that facilitate the prevention, identification, and correction of any errors in

[16] Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

protected information. The objective of these efforts is to ensure such information is accurate and not erroneously shared through the ISE. Further, each federal department and agency must ensure that when it is determined that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context, such that the rights of the individual may be affected, the potential error or deficiency must be communicated in writing to the other agency's privacy office.

(U) PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES PROTECTIONS

(U) Intelligence Community Privacy Policy

(U) Protecting privacy, civil rights, and civil liberties remains an ISE priority. Civil Liberties and Privacy Officers across all levels of government continue to oversee common ISE training, standards and activities to ensure compliance.

(U) In 2018, ODNI revised previous guidance and published a policy that addresses civil liberties and privacy as well as transparency.[17] The policy requires IC elements to ensure that civil liberties and privacy protections are integral considerations when planning and conducting intelligence activities. IC elements are also required to integrate, share, and safeguard information in a manner that protects civil liberties and privacy. Additionally, the policy institutionalizes the principle of providing greater transparency to the public, without causing damage to national security, to enhance understanding and trust concerning intelligence activities and the IC's governance framework. As such, the policy advises IC elements to support the robust implementation of the Principles of Intelligence Transparency for the Intelligence Community.

(U) Separately, ODNI's Office of Civil Liberties, Privacy, and Transparency (CLPT) is actively engaged with IC stakeholders in their ongoing efforts to fully implement all requirements mandated by EO 13587 including continued implementation of the ODNI insider threat program.[18]

(U) INFORMATION SECURITY PROTECTIONS

(U) Safeguarding Data

(U) The Intelligence Community (IC) continues to focus on executing the IC Directive (ICD) 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community, Strategic Implementation Plan*. ICD 501 implementation is linked to the IC's effort to adopt the IC Information Technology Enterprise, (ITE) and as a result, compliance with the ICD directly supports efforts to integrate and modernize the IC's information sharing and safeguarding environment.

[17] Intelligence Community Directive 107, Civil Liberties, Privacy, and Transparency, February 28, 2018

[18] EO 13587 - *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011

(U) Information that is relevant and usable by multiple entities must be discoverable, accessible, and usable, in a manner where data stewards can protect sources, methods, and activities, as well as reduce the risk of unauthorized or unintentional disclosure. Data stewards are responsible for evaluating the risks associated with providing information against the risks associated with denying requests for information.

(U) To facilitate data migration in 2017, the IC established and chartered the IC Chief Data Officer Council (CDOC). The IC CDOC facilitates and supports achievement of information sharing and safeguarding in conjunction with the IC Information Sharing and Safeguarding Executive and the Information Sharing Steering Committee by serving as a key collaboration forum to achieve those objectives. The IC CDOC serves as the IC's strategic enterprise data governance body, and worked in conjunction with ODNI to publish the first IC Information Environment (IE) Data Strategy.

(U) The IC IE Data Strategy is intended to guide the IC toward a common, more secure, and more integrated enterprise by leveraging the vision and framework of the IC IE to operationalize a data-centric community.

(U) IC IE Data Strategy Strategic Goals

(U) Develop and institutionalize a strategic data framework across the multi-fabric IC Information Environment.

(U) Ensure data is appropriately protected, shared, and handled across all fabrics.

(U) Create, resource, and leverage secured, scalable shared data services that meet the IC's needs for variety, velocity, volume, and veracity.

(U) Champion a culture that encourages and rewards data-centric behaviors, and effectively balances sharing and safeguarding.

(U) The Data Strategy encourages the IC to embrace a more disciplined approach to intelligence integration by ensuring that data is sharable, discoverable, accessible, retrievable, and protected. All of the strategic goals are in direct support of Information Safeguarding.

(U) Advancing Cybersecurity

(U) The far-reaching cybersecurity incidents of 2017 demonstrate that the Nation cannot ignore the impact of poor cybersecurity practices. These incidents demonstrate that effective cybersecurity protection requires any organization — whether a Federal agency or a public or private company — to identify, prioritize, and manage cyber risks across its enterprise.[19]

(U) In response, the President signed EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, to enhance cybersecurity risk management practices across the Federal Government. EO 13800 recognizes that the Government must ensure that it can secure citizens' information and that agencies can deliver on their core missions and services even as malicious cyber actors seek to disrupt those services. Accordingly, EO 13800 required every agency to conduct comprehensive reviews of their cybersecurity programs.

[19] Executive Office of the President, Federal Information Security Management Act, Annual Report to Congress, FY17

(U) While EO 13800 is the catalyst for securely modernizing Federal IT systems over the coming years, OMB and DHS's long-running efforts to instill disciplined cyber practices across government helped safeguard agency IT systems in the past year. As an example, DHS's efforts ensured that Federal agencies had already patched their IT systems to protect against ransomware attacks. Agencies also expanded their use of continuous monitoring tools and multi-factor authentication Personal Identity Verification (PIV) cards throughout the year.

(U) Within the IC, in 2017, the IC Security Coordination Center deployed the IC Analysis and Signature Tool (ICOAST) to increase sharing of cybersecurity threat intelligence including indicators of compromise (IoCs) and malware signatures across the IC information environment. Since ICOAST's deployment, over 450 cyber analysts from 85 IC and other federal departments and agencies have adopted the ICOAST capability and have contributed over 120K IoCs to date. As a result, IC cyber analysts are able to more rapidly deploy cybersecurity capabilities to enable analytic collaboration across the IC.

(U) WAY AHEAD

(U) The U.S. Government's ability to effectively share terrorism-related information and other information related to multiple threat actors, as well as their networks, and then use that information to support a broad array of national security related missions and activities is essential in protecting the homeland.

(U) As terrorism-related information sharing among key federal departments and agencies has matured, ISE partners are continuing to expand and promote collaboration on homeland security information sharing initiatives with state, local, tribal, and private sector partners. PM-ISE, in collaboration with the members of the Information Sharing Council, will continue promoting the use of interoperable systems, such as N-DEx, RISS and HSIN Exchange, and providing best practices for sharing terrorism-related and homeland security information.

(U) In collaboration with our federal partners, PM-ISE is devising ways to assess the effectiveness of the ISE on terrorism information sharing and in an effort to determine if the lessons learned can be applied to address other threats to the homeland. Further, PM-ISE is developing performance metrics for information-sharing initiatives used by various stakeholders to receive and share information across SBU networks.

(U) While the ISE was originally conceived to address the information sharing gaps that contributed to the terrorist attacks on 9/11, the attributes of the ISE, as established in the IRTPA, apply equally to the rapidly changing nature of all our national security related threats. As the Nation confronts new threats, PM-ISE, through the Information Sharing Council and consistent with the IRTPA, will assess and recommend whether or not, and by which means, the ISE should be expanded to allow the future integration of other relevant categories of information.

(U) APPENDIX A - ACRONYMS

AEP	Analytic Exchange Program
ATS-G	Automated Targeting System
BITMAP	Biometric Identification Transnational Migration Alert Program
BDSP	Biometric Data Sharing Program
CBP	Customs and Border Protection
CDOC	Chief Data Officer Council
CLPT	Civil Liberties, Privacy, and Transparency (ODNI)
CT	Counterterrorism
CT/CVE	Bureau of Counterterrorism and Countering Violent Extremism (DOS)
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOS	Department of State
EEI	Enhanced Engagement Initiative
EPIC	El Paso Regional Intelligence Center
ESTA	Electronic System for Travel Authorization
FBI	Federal Bureau of Investigation
FSLT	Federal, State, Local, and Tribal
FTF	Foreign Terrorist Fighters
FY	Fiscal Year
GAO	Government Accountability Office
GTAS	Global Travel Assessment System
HIDTA	High Intensity Drug Trafficking Area
HSIN	Homeland Security Information Network (DHS)
HSPD	Homeland Security Presidential Directive
I&A	Intelligence and Analysis (DHS)
IC	Intelligence Community
ICAM	Identity Credential and Access Management
ICD	Intelligence Community Directive

ICE	U.S. Immigration and Customs Enforcement
IDENT	Automated Biometric Identification System (DHS)
IE	Information Environment
IED	Improvised Explosive Device
INA	Immigration and Nationality Act
INTERPOL	International Criminal Police Organization
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISC	Information Sharing Council
ISE	Information Sharing Environment
IT	Information Technology
JCAT	Joint Counterterrorism Assessment Team
JTTF	Joint Terrorism Task Force
KFE-E	Kingfisher Expansion ESTA
KST	Known or Suspected Terrorist
N-DEx	National Data Exchange (FBI)
NCTC	National Counterterrorism Center
NFCA	National Fusion Center Association
OBIM	Office of Biometric Identity Management (DHS)
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PCSC	Preventing and Combating Serious Crime
PM-ISE	Program Manager, Information Sharing Environment
RFI	Request for Information
RISS	Regional Information Sharing System
SBU	Sensitive But Unclassified
SRTP	Secure Real-Time Platform (DHS)
TRIP	Traveler Redress Inquiry Program (DHS)
TSC	Terrorist Screening Center
USG	United States Government
VWP	Visa Waiver Program