

December 2016

REVIEWING THE DEPARTMENT OF HOMELAND SECURITY'S INTELLIGENCE ENTERPRISE

HOUSE HOMELAND SECURITY COMMITTEE MAJORITY STAFF REPORT



HOMELAND SECURITY
COMMITTEE

Table of Contents

I. Key Findings	3
II. Key Recommendations	4
III. Methodology and Acknowledgements	7
IV. Intelligence Enterprise Governance and Structure	8
V. Component Intelligence Program Missions and Structures	14
VI. Intelligence Enterprise Information Sharing within the Federal Government	25
VII. Intelligence Enterprise Sharing with State and Local Authorities	39
VIII. Conclusion	48
<hr/>	
Appendix I: Intelligence Enterprise Systems and Products	49
Appendix II: Acronyms and Abbreviations	56
Appendix III: Outside Groups Consulted	59
Appendix IV: Sources	59
<hr/>	

I. Key Findings

The attacks of September 11, 2001 (9/11) spurred Congress to create the Department of Homeland Security (DHS). Its purpose, in part, was to help unify “the many participants in the counterterrorism effort and their knowledge in a network-based information sharing system that transcends traditional government boundaries,” which would become one of the key recommendations of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission).¹ In pursuit of this goal, the DHS Intelligence Enterprise (IE) gradually evolved out of the relevant offices and functions of the 22 previously independent entities that eventually formed DHS. Although the IE has made progress unifying the U.S. government’s efforts to prevent terrorist attacks against the homeland, a 2014 RAND Corporation report accurately surmised that, despite an “intense focus on information sharing, the ability to fairly and accurately measure the value of these – sometimes expensive – efforts remains limited.”² Partly as a result, the Majority Staff of the House Homeland Security Committee conducted a review of terrorism-related intelligence sharing throughout the DHS IE, finding that:

1. DHS has made significant strides in improving the flow of terrorism information to all stakeholders since its creation.
2. The DHS IE is an evolving structure, and the authority of the Chief Intelligence Officer (CINT) is not completely accepted throughout the IE.
3. Some DHS IE members do not have clear, or even explicitly identified, missions. This vagueness causes overlapping efforts and inhibits the effective sharing of terrorism-related intelligence due to the fact that information flows are sometimes unclear.
4. The DHS IE does not have a consolidated intelligence doctrine and the CINT does not have full awareness of all terrorism-related intelligence sharing agreements into which the various DHS Components have entered. As a result, personal, rather than institutional, relationships play a major role in determining the effectiveness or ineffectiveness of intelligence sharing within and between federal and non-federal entities.
5. The DHS IE employs a vast array of Information Technology (IT) systems that require standardization and modernization. Implementing the DHS Data Framework initiative is a critical project which will help ameliorate this issue, while also allowing for more effective intelligence analysis of Departmental data.
6. Members of the DHS IE generate a vast array of finished intelligence products. These are often nothing more than a repackaging of products from statutory Intelligence Community (IC, defined by the National Security Act of 1947, as amended) members, rather than analyses of DHS-derived information. Synthesizing such data into intelligence products primarily using Department-specific information is one of the unique contributions the IE can make to our nation’s security. Conversely, large amounts of this raw information of potential intelligence value are not easily accessible to relevant stakeholders in DHS, the IC, or State, local, tribal, and territorial (SLTT) law enforcement organizations.

II. Key Recommendations

SECRETARY OF HOMELAND SECURITY

1. Re-issue the directive defining the DHS IE, explicitly identifying which Components are part of it. Furthermore, the directive should explicitly identify all personnel conducting intelligence activities as being part of the Component's (single) Intelligence Program.
2. Issue a policy directive clearly separating the functions of the CINT and the chief of DHS' Office of Intelligence & Analysis (I&A).
3. Issue a policy directive more clearly defining the relationship between the CINT, I&A, and the other organizations in the Department conducting intelligence activities.

CHIEF INTELLIGENCE OFFICER, DEPARTMENT OF HOMELAND SECURITY

4. Create a mechanism for coordinating policy proposals with the Components, giving them time to comment and raise objections prior to the issuance of Departmental directives, using the Homeland Security Intelligence Council towards this end.
5. In coordination with the Secretary, review I&A's legislative charter to ensure it has the authorities necessary to face both current and projected threats to the homeland. Report to Congress any relevant legislative recommendations that result.
6. More closely examine the CINT's relationship with the Federal Emergency Management Agency (FEMA), and that organization's interaction with the broader IE.
7. More thoroughly integrate the Office of Operations Coordination into the IE, especially with regard to dissemination of information of potential intelligence value derived from open sources and SLTT law enforcement organizations.
8. Conduct a detailed review of all intelligence rotational programs for which IE employees are eligible, standardizing, consolidating, and tracking the various programs to the greatest extent feasible.
9. With the support of the Secretary, more aggressively enforce the CINT's mandate to coordinate and approve all memoranda of understanding, and maintain an up-to-date list of all relevant intelligence-sharing agreements.
10. Standardize raw intelligence reporting formats throughout the Department and create a system of record for dissemination, discoverable by all personnel with a need-to-know, even for products containing information that does not meet the standard for national intelligence reporting.
11. Ensure these raw intelligence reporting formats allow for segregation of sensitive data from less critical information, and ensure said formats are compatible with and easy to manipulate via the DHS Data Framework.

12. Use existing legal authorities to standardize methods for collecting open source information and disseminating reporting derived from it throughout the IE.
13. Review existing IC open source collection and analysis capabilities and determine whether the DHS IE can use some of these resources instead of pursuing similar initiatives “in-house.”
14. Ensure that all appropriately cleared SLTT officials with a need-to-know can access relevant IC-created intelligence products to the extent practicable, rather than repackaging these products and disseminating them directly.
15. Conduct an audit of all contractors conducting open source analysis throughout the DHS IE, and consolidate their efforts as much as possible.
16. Standardize all IE analytical product formats where practicable.
17. Develop a plan to incentivize and evaluate the use of Department-derived information in the analytical products of all IE members as appropriate.
18. Issue an intelligence “discoverability” directive similar to Intelligence Community Directive 501.
19. Develop and issue a Departmental Intelligence Doctrine, using relevant Component policies and IC Directives as a starting point.
20. Aggressively incorporate new data into the DHS Data Framework, and ensure that all Component Intelligence Programs both contribute their data sets and employ the system to the utmost of their abilities.
21. Develop a consistent methodology for measuring the IE’s effectiveness with regard to sharing intelligence with all SLTT authorities nationwide.
22. Develop a strategic plan for engagement with State and local fusion centers that includes all Component Intelligence Programs and focuses on producing timely, actionable intelligence, rather than sheer numbers of reports. This plan should include a revised method for evaluating fusion centers on the same criterion.
23. Develop a comprehensive strategy for intelligence sharing and engagement with the following entities: Joint Terrorism Task Forces, Field Intelligence Groups, Regional Information Sharing System Centers, and Organized Crime Drug Enforcement Task Forces under the control of the Department of Justice; Field Intelligence Groups administered by Customs and Border Protection (CBP); Field Offices of the Bureau of Immigration and Customs Enforcement (ICE); and High Intensity Drug Trafficking Areas Investigative Support Centers operating under the auspices of the Office of National Drug Control Policy.
24. Direct I&A to identify explicitly which fusion centers have FBINet and Guardian Access, and engage with the FBI to ensure more widespread fusion center analyst access to the Guardian system.

25. Ensure cross-compatibility between, or at least maximum possible fusion center access to, both FBI Net and the Homeland Secure Data Network.
26. Determine exactly how IE members use the Homeland Security Information Network, specifically with regard to sharing with SLTT authorities.
27. Develop an Enterprise-wide policy for what products the Component Intelligence Programs should post to the Homeland Security Information Network, and how they use the platform to collaborate with SLTT authorities.
28. Conduct a review to ensure that all IE systems, and to the extent possible, those of SLTT partners, are interoperable with all relevant federally-funded databases containing terrorism information, especially those of the Department of Justice.

DEPARTMENT OF HOMELAND SECURITY COMPONENT HEADS

29. I&A should create an **Office of Strategic Intelligence** to work closely with other Components, SLTT law enforcement authorities, and the IC to identify emerging threats to the homeland.
30. CBP, the Transportation Security Administration (TSA), and United States Citizenship Immigration Services (USCIS) should each consolidate their respective intelligence functions into one Component Intelligence Program per entity.
31. FEMA should more tightly define its Component Intelligence Program mission statement.
32. The Office of the Chief Security Officer (OCSO) should more tightly define its mission statement.
33. All Components should produce the minimum number of different formats of finished intelligence as is necessary.
34. All Components should buy commercial subscriptions for open source analysis when appropriate, rather than hiring contractors to produce similar material.

III. Methodology and Acknowledgements

The Committee conducted this review from December 2015 through August 2016. It consisted of three stages. During the first, Committee staff met with former DHS officials, outside groups, and non-DHS federal government organizations that had previous experience in evaluating intelligence sharing (see Appendix III for a full list). The Committee is deeply grateful for the assistance of these outside experts. These groups assisted in refining our methodology and the questionnaire we sent to DHS IE members. We also held meetings with the DHS Under Secretary for Intelligence and Analysis/Chief Intelligence Officer and his staff to develop a baseline understanding of the state of terrorism-related intelligence sharing in the Department, and briefed them on our plans for this review.

The second stage of this review comprised sending a detailed set of questions to all offices comprising the DHS IE, and reviewing a broad array of raw and finished intelligence reporting created by each organization. The Department was generally receptive to our efforts, with some exceptions. Under Secretary for Intelligence and Analysis Francis Taylor and his staff were especially helpful, and we appreciate his efforts in facilitating Congressional oversight. We also met with a variety of STLL law enforcement organizations and their representatives to evaluate the DHS IE from the perspective of its most critical partners.

The third stage of our review consisted of follow-up information requests, interviews, and research, culminating with the writing and release of this report. We requested additional briefings from the DHS Components for whom we had especially complex or detailed questions, and integrated their responses into our report. The Committee also provided a draft copy of this document to all members of the DHS IE, allowing them time to comment on our findings, and incorporated their responses when appropriate.

DEFINITIONS AND SCOPE

For the purposes of this report, the Committee will use the DHS definition of “intelligence,” which is “[i]nformation that has tactical, operational, or strategic value” including “foreign intelligence and counterintelligence.”³ The term “Components” will refer to the DHS’ self-described “Operational and Support Components,” as well as to the OCSO, which is part of the Department’s Directorate for Management.⁴

Although the Committee fully understands that DHS’ mission includes much more than just counterterrorism (CT), this report will focus on this topic specifically. The definition of “terrorism,” for the purposes of this study, is almost identical to that found in Title 18 of United States Code, referring to “violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State” and “appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping.”⁵ Finally, although engagement with the private sector is a significant part of DHS’ mission, its interactions with non-governmental entities are outside the scope of this report. The Committee will examine these relationships further in depth in a subsequent study.

IV. Intelligence Enterprise Governance and Structure

BACKGROUND

Prompted by the 9/11 terrorist attacks, Congress created DHS via the Homeland Security Act of 2002. This legislation made the principle mandate of the Department “to prevent terrorist attacks within the United States.”⁶ Creating the Department was an effort to address a problem that the 9/11 Commission would later identify: the “national intelligence structure is still organized around the collective disciplines of the home agencies, not the joint mission.”⁷ To remedy this organizational failure and fulfill the Department’s founding charter, the Homeland Security Act also created within the Department a “Directorate for Information Analysis and Infrastructure Protection headed by an Under Secretary.” This Directorate – abbreviated “IAIP” – had the mission of receiving and analyzing intelligence from U.S. government agencies at the federal, state, and local levels so as to “identify and assess the nature and scope of terrorist threats to the homeland.”⁸

Under the direction of Secretary of Homeland Security (Secretary) Michael Chertoff, DHS began a Second Stage Review (2SR) in 2005. The goal of 2SR was to conduct “a systematic evaluation of the Department’s operations, policies and structures.”⁹ As a result of the review’s findings, Secretary Chertoff reorganized the Directorate for IAIP, transferring its information analysis responsibilities to the newly-created I&A. At the head of I&A, Secretary Chertoff designated an Assistant Secretary for Information Analysis who would also serve as the Department’s CINT.¹⁰ The Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act) codified this organizational change, charging I&A with the responsibility “to review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information” in an effort to ameliorate the “structural barriers to performing joint intelligence work” that the 9/11 Commission deplored.¹¹ The head of I&A, which the 9/11 Commission Act elevated to the level of Under Secretary for Intelligence and Analysis (U/SIA), would similarly “serve as the Chief Intelligence Officer of the Department.”¹²

THE HOMELAND SECURITY INTELLIGENCE COUNCIL

The CINT chairs the Homeland Security Intelligence Council (HSIC), which is “an advisory body chaired by the CINT and consisting of other senior officials within [I&A], the [Key Intelligence Officials (KIO)], and other Department officials as invited by the CINT,” according to DHS policy.¹³ KIOs are direct representatives of Component heads who serve as their emissaries on the HSIC.¹⁴ Established in 2006, the CINT uses the HSIC to issue “instructions, processes, standards, guidelines, procedures, strategies, budget guidance, and other implementing policy guidance.”¹⁵ Although DHS policy only specifies that the HSIC meet at “regular intervals,” as of early August 2016 it was meeting approximately every two weeks.¹⁶

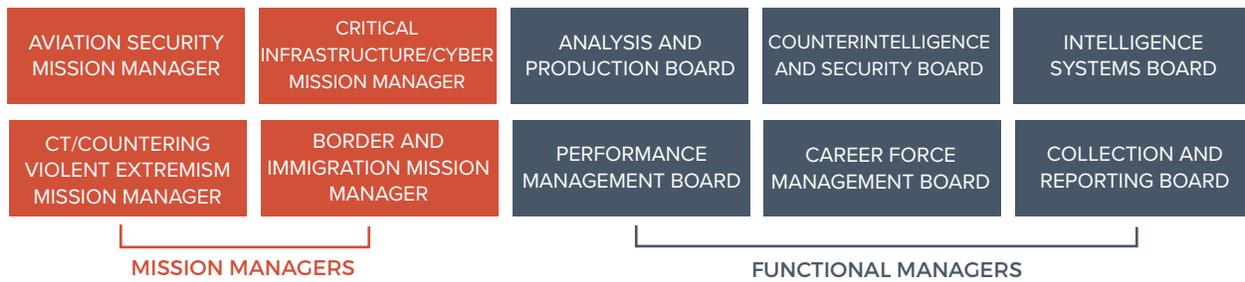
Members of the Homeland Security Intelligence Council

Official	Component / Office
Under Secretary for Intelligence and Analysis (Chair)	Intelligence & Analysis
Principal Deputy Under Secretary for Intelligence and Analysis	Intelligence & Analysis
Assistant Commandant for Intelligence/Criminal Investigations	Coast Guard
Deputy Under Secretary	National Protection and Programs Directorate
Assistant Commissioner for Office of Intelligence	Customs and Border Protection
Assistant Administrator for Intelligence and Analysis	Transportation Security Administration
Assistant Director for Intelligence	Immigration and Customs Enforcement
Associate Director for Fraud Detection and National Security	Citizenship and Immigration Services
Deputy Administrator for Protection and National Preparedness	Federal Emergency Management Agency
Assistant Director for Strategic Intelligence and Information	United States Secret Service
Chief Security Officer	Office of the Chief Security Officer
Director, Office of Operations Coordination	Office of Operations Coordination
Associate General Counsel for Intelligence	Office of the General Counsel

Source: DHS, "Homeland Security Intelligence Counsel Charter," September 2015

In February 2016, the CINT created a set of Intelligence Mission Managers (IMM) and Intelligence Functional Managers (IFM) to support the HSIC.¹⁷ This structure is roughly analogous to how the Director of National Intelligence (DNI) uses National Intelligence Managers to run the IC. KIOs from the relevant Components nominate Mission Managers to serve on the HSIC.¹⁸ Although originally all IFM were I&A employees, as of July 2016 both OCSO and CBP personnel filled some of these roles.¹⁹

MISSION / FUNCTIONAL MANAGER FRAMEWORK



Source: CINT document provided to Committee, December 14, 2015

The Committee heard relatively uniform praise throughout DHS IE with regard to the HSIC construct. CBP officials were appreciative of being able to take the lead on certain topics such as border security, working under the HSIC structure.²⁰ TSA officials were especially supportive of the Mission Manager concept, which allowed for subject matter experts to lead analytical efforts in their particular fields of expertise.²¹ Although there is no explicit statutory charter for it, the HSIC appears to be performing a useful coordinating role, and the Committee recommends DHS take no action with regard to its structure or composition.²²

THE INTELLIGENCE ENTERPRISE

The Department's early intelligence activities had "no vision, mission statement, concept of operations, well-defined budget, or information practices" in the words of one former U/SIA.²³ DHS' intelligence coordination and dissemination practices have thus come a long way since that point. Although not defined by statute, DHS uses the concept of the IE when discussing its broad intelligence activities.²⁴ By statute, the U/SIA is "dual-hatted" as the head of I&A and as the CINT, who leads the IE.²⁵ DHS elaborates on the role of the CINT with regard to the IE via Departmental policy, identifying him as "the DHS official who exercises leadership and authority over Intelligence policy and programs DHS-wide in partnership with heads of the Components." There is, however, significant confusion throughout DHS – at both the headquarters and Component levels – as to exactly which Components are part of the Intelligence Enterprise.

The Department's early intelligence activities had "no vision, mission statement, concept of operations, well-defined budget, or information practices."

CHARLES ALLEN, FORMER UNDER SECRETARY FOR INTELLIGENCE AND ANALYSIS

February 1, 2016

The Department has drafted a variety of documents which define the IE in different ways, and understanding of its composition varies greatly throughout the Department. Employees from two Components who briefed the Committee, for example, did not appear to know of the existence of the IE, initially assuming it was synonymous with the broader

IC.²⁶ The CINT's dedicated staff (CINT Staff) provided a document to the Committee in late 2015 depicting the IE as comprising I&A, the United States Coast Guard (USCG), National Protection and Programs Directorate (NPPD), CBP, TSA, ICE, USCIS, FEMA, the United States Secret Service (USSS), OCSO, and the Office of Operations Coordination (OPS).²⁷ A 2014 GAO report, analyzing DHS-provided information, identified the IE as comprising the same members.²⁸ A CINT Staff member later verbally characterized OPS and the OCSO as "ex officio" members.²⁹ Upon review of a draft of the Committee's report, however, the CINT staff wrote to the Committee that "USSS, OPS and OCSO are not part of the IE."³⁰ USSS and OCSO legislative affairs personnel similarly denied that they were members.³¹ OPS, however, asserted that it was a member.³² A separate DHS document, released in February 2016, identifies IE members as the "intelligence offices" of CBP, ICE, USCIS, USCG, TSA, USSS, and FEMA (excluding I&A, NPPD, OCSO, and OPS).³³ The DHS Management Directive defining the IE is also vague with regard to identifying exactly which organizations are part of it. The document describes the IE as being "led by the CINT and consisting of the [Component Intelligence Programs] of DHS Intelligence Components."³⁴

The aforementioned definition of the IE refers to two other entities: "Intelligence Components" and "Component Intelligence Programs." Echoing the 9/11 Commission Act, Departmental policy describes an "Intelligence Component" as any "Component or Entity of the Department that collects, gathers, processes, analyzes, produces, or disseminates Intelligence Information within the scope of the Information Sharing Environment except (1) the United States Secret Service and (2) the Coast Guard, when operating under the direct authority of the Secretary of Defense or Secretary of the Navy."³⁵ This definition in particular did not appear to cause significant confusion, mainly because the Committee rarely identified any DHS employees or entities using it. The term Component Intelligence Program (CIP), however, is more contentious.³⁶ According to DHS policy, CIPs are "any organization within a DHS Intelligence Component, a significant purpose of which is the collection, gathering, processing, analysis, production, or dissemination of intelligence," or which employs intelligence professionals (of the 0132 job series) to perform "National or Departmental Intelligence functions."³⁷ A senior CINT Staff member, however, provided a different characterization, explaining that CIPs are "any organization that conducts the complete intelligence cycle."³⁸

The various DHS Components define their CIPs in a variety of ways. CBP, in addition to its CIP, the Office of Intelligence (OI), has three distinct subcomponents which conduct intelligence activities: the Office of Field Operations' (OFO) National Targeting Center (NTC), United States Border Patrol's (USBP) Sector Intelligence Units, and the Air and Marine Operations (AMO) Intelligence Directorate.³⁹ CBP officials did not consider these three organizations to be part of the same CIP as OI, and it remains an unresolved question as to whether they constitute additional CIPs themselves.⁴⁰ TSA OIA maintains a total of almost 735 Full Time Equivalent (FTE) employees, including its field-based officers.⁴¹ TSA, however, only considers 237 of these personnel – all of those in the 0132 job series – to be members of its CIPs.⁴² Furthermore, inside OIA, TSA has designated three different CIPs.⁴³ USCIS considers its counterintelligence/security functions as well as its field operations to comprise separate CIPs outside of its Fraud Detection and National Security (FDNS) Directorate, telling the Committee that it also maintains three CIPs.⁴⁴ ICE, conversely,

considers its CIP to include anyone involved in intelligence activities across the entire organization. All personnel with the GS-0132 (intelligence series) designation, and any GS-1811 (criminal investigation series) personnel involved in intelligence, thus fall under the authority of ICE's KIO.⁴⁵

CINT Staff members told the Committee in January 2016 that the CINT had tasked the Components to identify their CIPs.⁴⁶ As of August 2016, the process was ongoing.⁴⁷ The Committee learned that, as a result of the aforementioned lack of clarity with regard to exactly what comprises a CIP, there was still debate as to the total number of CIPs in the Department. The CINT Staff's August 2016 estimate ranged from 12 to 15, depending on how CBP and USCIS categorized their respective separate intelligence offices.⁴⁸ The Committee views a more expansive definition, such as that which ICE uses, as more useful and coherent. This "one CIP per Component" construct allows for standardization of policies and procedures, allows for more streamlined and effective oversight, and generally improves unity of effort. Throughout this report, however, the term "CIP" will refer to those organizations explicitly defined as such by the DHS Component in question.⁴⁹

Recommendation: The Secretary should re-issue the directive defining the DHS Intelligence Enterprise, explicitly identifying which Components are part of it. Furthermore, the directive should explicitly identify all personnel conducting intelligence activities as being part of the Component's (single) CIP.

COMPONENT RELATIONSHIPS WITH THE CHIEF INTELLIGENCE OFFICER

Despite its more than 10 years of existence, the DHS IE is still experiencing growing pains. A clear tension exists between the Components and the CINT, as well as to a lesser extent, between other Components and I&A. The CINT Staff has been conducting in-depth, annual reviews with each CIP since 2006, and this process has clearly revealed significant room for improvement with regard to general IE governance.⁵⁰ CINT Staff members expressed their perception to the Committee that, unless an agency or Component head wanted to implement a specific policy, the Component was unlikely to do so.⁵¹ More diplomatically, U/SIA Taylor told the Committee that there was "mixed" CIP investment in terms of participating in the IE, with some being reticent towards complying with DHS headquarters directives. He told the Committee that he had observed "slow-rolling" from some Components, but not outright "defiance."⁵²

The Committee similarly detected a wide disparity throughout the Department with regard to acquiescence to the CINT's authority. When asked by the Committee what his organization would do if the CINT issued a policy or mandate with which he disagreed, a senior DHS Component official candidly admitted that he would "just ignore it." Only direct intervention from the Secretary would compel compliance from this particular official.⁵³ Conversely, a senior official from the Threat Management Division (TMD) of NPPD's Federal Protective Service (FPS) told the Committee that "everything we do is under the authority" of the CINT.⁵⁴ Other Components took more nuanced positions. TSA viewed its relationship with the CINT as having improved over time, and was appreciative that the CINT would advocate for access to certain information on TSA's behalf.⁵⁵ ICE Homeland

Security Investigations-Intelligence (HSI-Intel) officials told the Committee that they felt there was a lack of clear differentiation between the CINT and I&A, causing some friction. In their view, I&A employees occasionally saw themselves as “above” the Components and willing to dictate policies to them using the CINT’s authority.⁵⁶

The most common complaint the Committee heard with regard to the CINT structure was its apparent heavy-handedness. To some CIP officials, Department level directives occasionally did not appear to have been coordinated and thought through, often making unrealistic demands of the Components.⁵⁷ Other DHS personnel similarly resented under- or un-funded requirements to implement new systems and policies, which represented general lack of understanding of the situation at the ground level, in their view.⁵⁸ Despite some tension between the CINT and the Components, the Committee views these issues as unrelated to U/SIA Taylor himself. CIP officials generally praised his competence and professionalism; TSA officials in fact acknowledged that U/SIA Taylor had done more work to improve the functioning of the DHS IE than any of his predecessors.⁵⁹

Recommendation: The Secretary should issue a policy directive more clearly separating CINT and I&A functions.

Recommendation: The Secretary should issue a policy directive more clearly defining the relationship between the CINT, I&A, and the other organizations in the Department conducting intelligence activities.

Recommendation: The CINT should create a mechanism for coordinating policy proposals with the Components, giving them time to comment and raise objections prior to the issuance of Departmental directives, using the HSIC towards this end.

Examples of the practical consequences of these disputes abound. For example, the CINT requires that all Components route all Requests for Information (RFI) to the IC via I&A, having recently instituted a Department-wide RFI policy.⁶⁰ Due to the delays that occasionally result from such review, however, some Components simply make their requests directly to the relevant IC organization.⁶¹ Policies associated with coordinating intelligence-sharing Memoranda of Understanding (MOU), detailed later in this report, highlight another result of the aforementioned tension.

More significantly than MOU and RFI management, one Component is pursuing its own relationship with the IC, partially independently from the CINT. As of early March 2016, CBP was reportedly negotiating directly with the DNI to make its CIP a statutory member of the Intelligence Community, according to an outside observer familiar with the situation.⁶² CBP OI contested this assertion, however, telling the Committee that at the request of the DNI in January 2016, it began examining the merits of statutory membership to the IC and has coordinated analysis of potential membership with both the CINT and Department at large.⁶³ In addition to a legislative route, the President, or the DNI and the head of the agency in question, can administratively designate said organization as a member of the IC, according to Executive Order 12333, as amended (EO 12333).⁶⁴ When pressed by the Committee as to why they wanted to become an IC member, CBP officials expressed their

desire to “have a seat at the table,” exert more influence within the IC, and bring their “operational experience” to bear.⁶⁵

U/SIA Taylor observed that there might be some value for portions of CBP to become members of the statutory IC, but was concerned with the potential effects it might have on their ability to execute their border security mission, by forcing parts of the organization to comply with EO 12333.⁶⁶ According to this order, however, the DNI may “provide advisory tasking concerning collection and analysis of information or intelligence relevant to national intelligence or national security to departments, agencies, and establishments of the United States Government that are not elements of the Intelligence Community.”⁶⁷ This provision allows for the DNI to provide suggested collection priorities to CBP directly. Conversely, the CINT serves as an advocate for representing the DHS IE to the broader IC, consolidating all component concerns into a coordinated Department position. Due to the lack of any pressing need or convincing justification, the Committee opposes moving any part of CBP into the IC at this time.

V. Component Intelligence Program Missions and Structures

In addition to their exact number and composition being unclear, there are significant differences with regard to the missions of the DHS CIPs. The Committee requested mission statements from each of the ones we had identified as of March 2016, in order to better understand their functions.⁶⁸ An analysis of the results reveals a wide disparity in terms of specificity and scope. The Committee suspects that, for at least some CIPs, there existed no agreed-upon mission statement until the Committee requested it. Tighter mission statements could help the CIPs better coordinate their activities, reducing overlap and providing metrics by which they can evaluate their performance.

DHS Component	Component Intelligence Program	Mission Statement Provided to Committee
Intelligence and Analysis	Intelligence and Analysis	Equip the Homeland Security Enterprise with the intelligence and information it needs to keep the homeland safe, secure, and resilient.
United States Coast Guard	Coast Guard Intelligence	[C]onduct intelligence operations and activities to provide timely, relevant, and actionable intelligence to shape operations, planning, and decision making in support of Coast Guard and Homeland Security missions, and national security requirements.

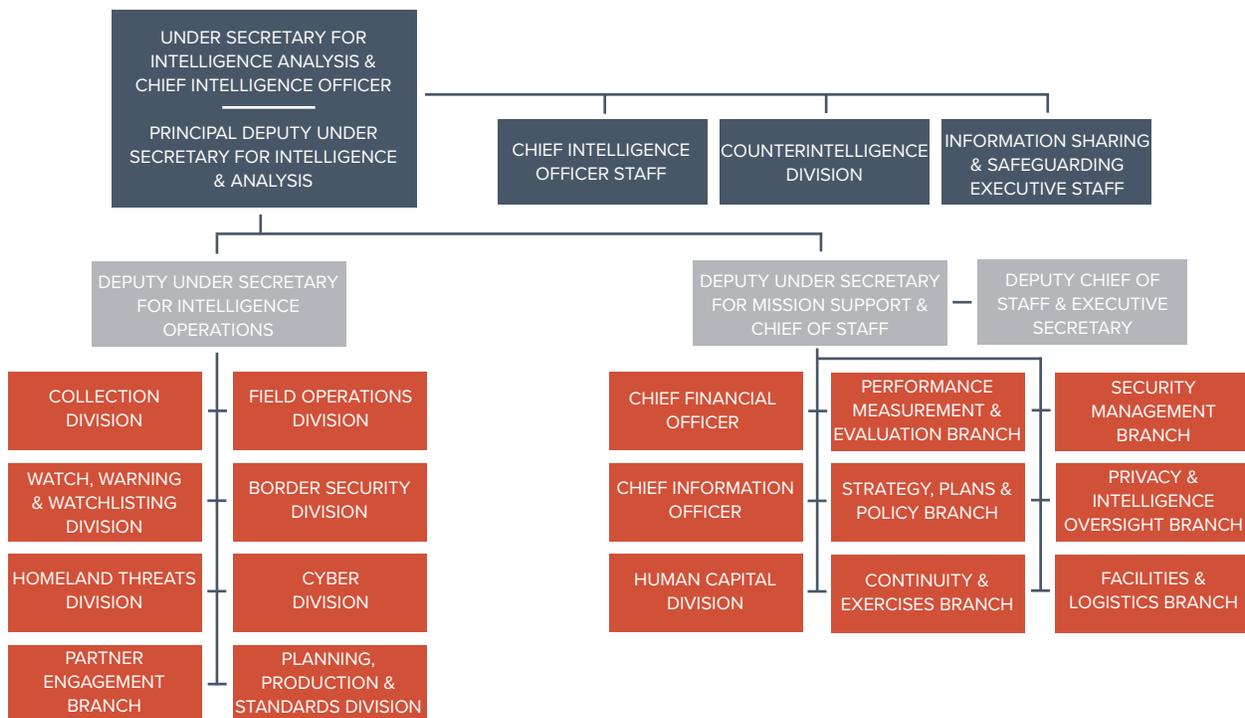
National Protection and Programs Directorate	Office of Cyber and Infrastructure Analysis Intel Support Branch	Coordinates Intelligence support to NPPD's critical infrastructure security and resilience mission.
	Federal Protective Service Threat Management Division	Provide Federal Protective Service stakeholders with threat-based, mission focused analysis of current and emerging threats to government facilities and their occupants through professionally managed and integrated threat management focused on reducing risk at government facilities.
Customs and Border Protection	Office of Intelligence*	[T]o develop, provide, coordinate, and implement intelligence capabilities to support the execution of CBP's primary mission – to secure America's borders while facilitating legitimate trade and travel. It focuses on full execution of the intelligence cycle to provide timely, accurate, relevant, and anticipatory intelligence supporting CBP decision makers, daily enforcement, and future operations.
TSA	Office of Intelligence and Analysis*	[T]o identify security risks and to prevent attacks against the transportation system.
Immigration and Customs Enforcement	Homeland Security Investigations - Intelligence	[C]ollecting and analyzing timely and accurate intelligence on illicit trade, travel, and financial activity with a United States nexus and sharing it with ICE HSI field offices and global law enforcement partners; [M]aintaining global situational awareness through the operation of a 24/7 watch that receives, coordinates, and disseminates classified and unclassified information, and facilitates the exchange of law enforcement and national intelligence between ICE directorates, ICE leadership, and the Department of Homeland Security (DHS); [E]stablishing and maintaining secure data communications connectivity agency-wide; and [P]roviding ICE with continuity of operations, emergency response, and crisis management plans so that it remains a resilient organization prepared for and able to respond to emerging threats and situations.
United States Citizenship and Immigration Services	Fraud Detection and National Security Directorate*	[I]nforms FDNS leadership and, when appropriate, USCIS senior leadership and other USCIS Directorates of intelligence and information on significant national security issues and threats; manages the processing, analysis, production, and dissemination of USCIS immigration database information and intelligence products which focus on enhancing national security efforts and identifying trend and patterns in immigration fraud; is the USCIS lead for coordinating information sharing and collaboration efforts between USCIS, DHS, and the Law Enforcement (LE) and IC; and facilitates the completion of Requests for Information (RFIs) received from external agencies.

Federal Emergency Management Agency	Protection and National Preparedness office	[D]issemination of time-sensitive information and intelligence information and the development of threat assessments based on access to relevant IC and OPEN SOURCE reporting that inform the situational awareness and decision making of FEMA Senior Leadership in the performance of FEMA's agency, departmental, and Federal Executive Branch roles, functions, missions, and activities, particularly during periods of catastrophic events, regardless of their source. Access to IC reporting is crucial.
United States Secret Service	Have not designated CIPs. Mission provided is either for entire organization or intelligence office	The USSS Protective Intelligence and Assessment Division "supports the agency's unique protective mission."
Office of the Chief Security Officer		Protection of personnel, information, facilities, property, equipment and other material resources.
Office of Operations Coordination Planning		[I]s a consumer of intelligence information, leveraging the work of the DHS Office of Intelligence and Analysis and other intelligence offices in order to enhance its own activities.

**As previously identified, the exact composition and number of CIPs for these Components is an unresolved issue. The Committee provides the missions for those organizations which each Component has explicitly identified as a CIP.*

Source: Correspondence with Component legislative affairs offices, April-June 2016

OFFICE OF INTELLIGENCE AND ANALYSIS



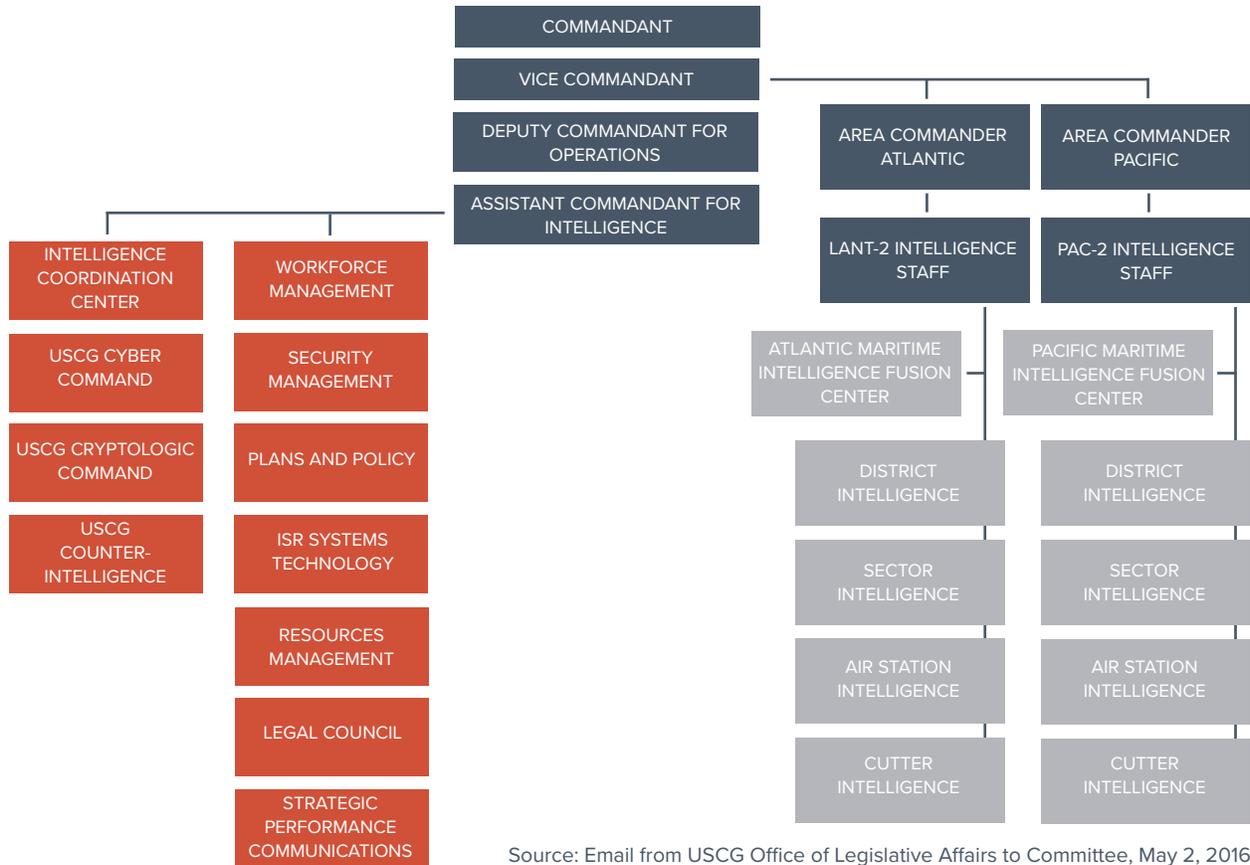
Source: Email from I&A Office of Legislative Affairs to Committee, June 30, 3016

I&A expounded on its relatively broad mission with a “vision,” which is to be “a premier intelligence enterprise that drives information sharing and delivers predictive intelligence and analysis to operators and decision makers at all levels.”⁶⁹ At least one outside group has suggested that Congress more tightly define I&A’s mission and review “the twenty-five I&A functions set out in the statute.”⁷⁰ It is possible that I&A’s vague mission reflects its rather expansive legislative charter.⁷¹ Furthermore, due to its primary statutory responsibility to “identify and assess the nature and scope of terrorist threats to the homeland,” I&A must allocate resources towards predicting future threats against the United States.⁷² Due to its role as both a member of the Intelligence Community and as the primary conduit for the federal government to receive SLTT information of potential intelligence value, I&A should dedicate analytical capacity towards long-term strategic efforts to identify emerging risks to homeland security. Not focused on normal day-to-day operations, this group would identify potential future threat actors, untapped data sets residing both inside and outside of the Department, and possible gaps in intelligence collection practices and analysis.⁷³

Recommendation: The CINT, in coordination with the Secretary, should review I&A’s legislative charter to ensure it has the authorities necessary to face both current and projected threats to the homeland. The CINT should report to Congress any relevant legislative recommendations that result.

Recommendation: I&A should create an Office of Strategic Intelligence to work closely with other Components, SLTT law enforcement authorities, and the IC to identify emerging threats to the homeland.

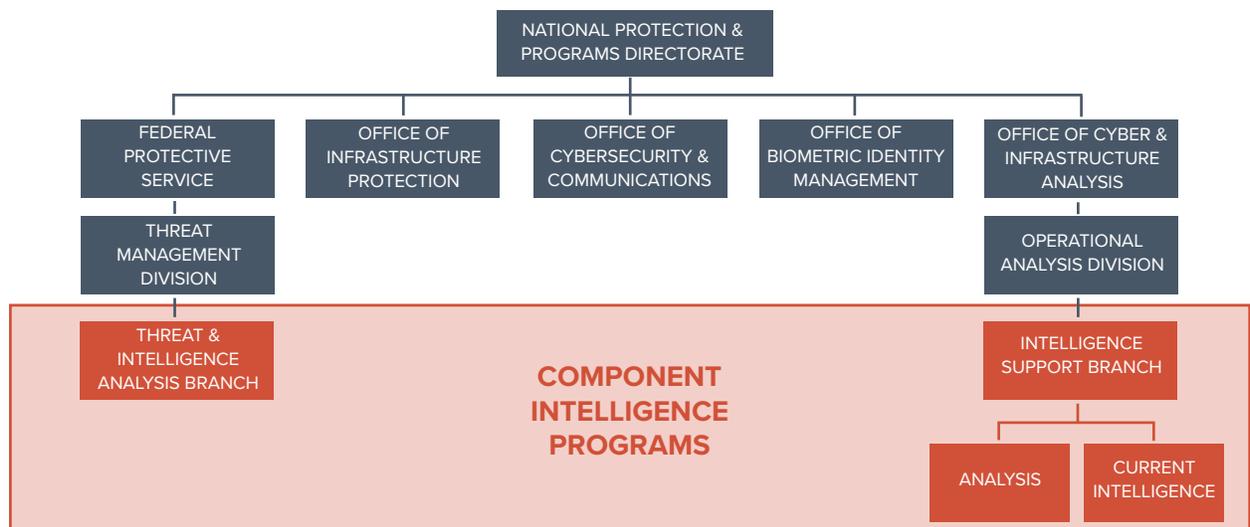
UNITED STATES COAST GUARD INTELLIGENCE



Source: Email from USCG Office of Legislative Affairs to Committee, May 2, 2016

The USCG Intelligence (USCG-Intel) mission was appropriately scoped, in the opinion of the Committee, and throughout our review of the DHS IE, we found the Coast Guard’s CIP to be especially well defined in terms of its roles and responsibilities. The intelligence products that the Committee reviewed focused heavily (and appropriately) on USCG activities.⁷⁴

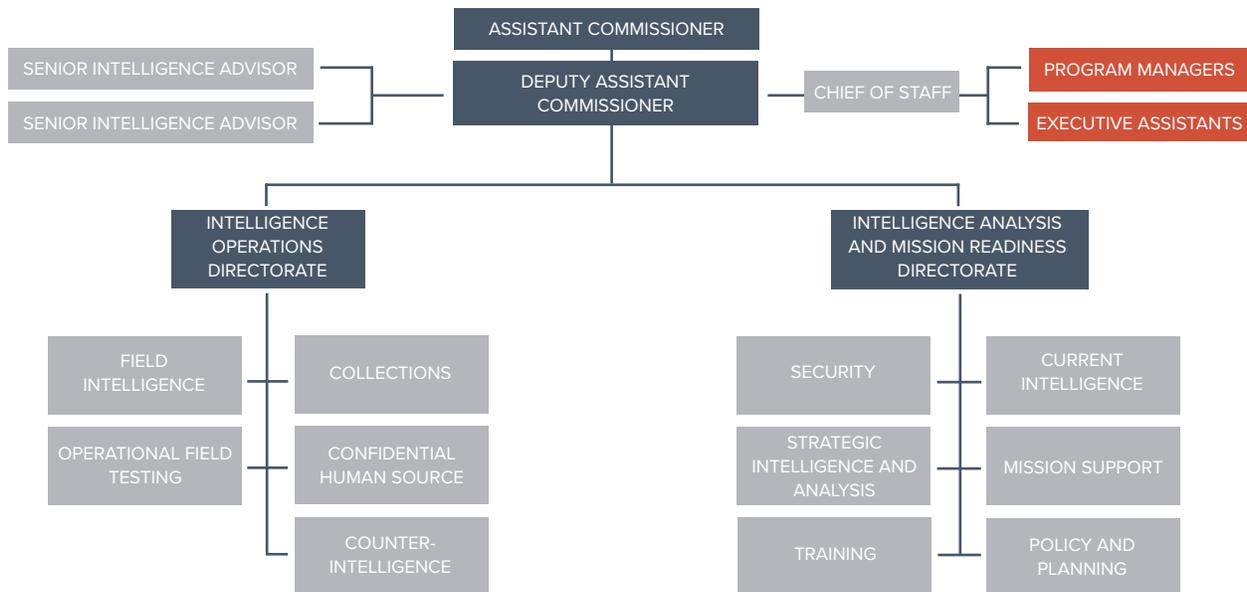
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE



Source: Email from NPPD Office of Legislative Affairs to Committee, July 25, 2016

NPPD has two CIPs: the Intelligence Support Branch under the Operational Analysis Division of the Office of Cyber & Infrastructure Analysis (OCIA-ISB) and the Threat and Intelligence Analysis Branch of FPS’s TMD (FPS-TMD).⁷⁵ As of the writing of this report, DHS had proposed an internal reorganization of NPPD and the Committee has pending legislation that would restructure the organization into the “Cybersecurity and Infrastructure Protection Agency.”⁷⁶ The reorganization efforts seek to elevate the focus on cyber-related missions, reduce management inefficiencies, and eliminate stovepipes.⁷⁷

CUSTOMS AND BORDER PROTECTION, OFFICE OF INTELLIGENCE



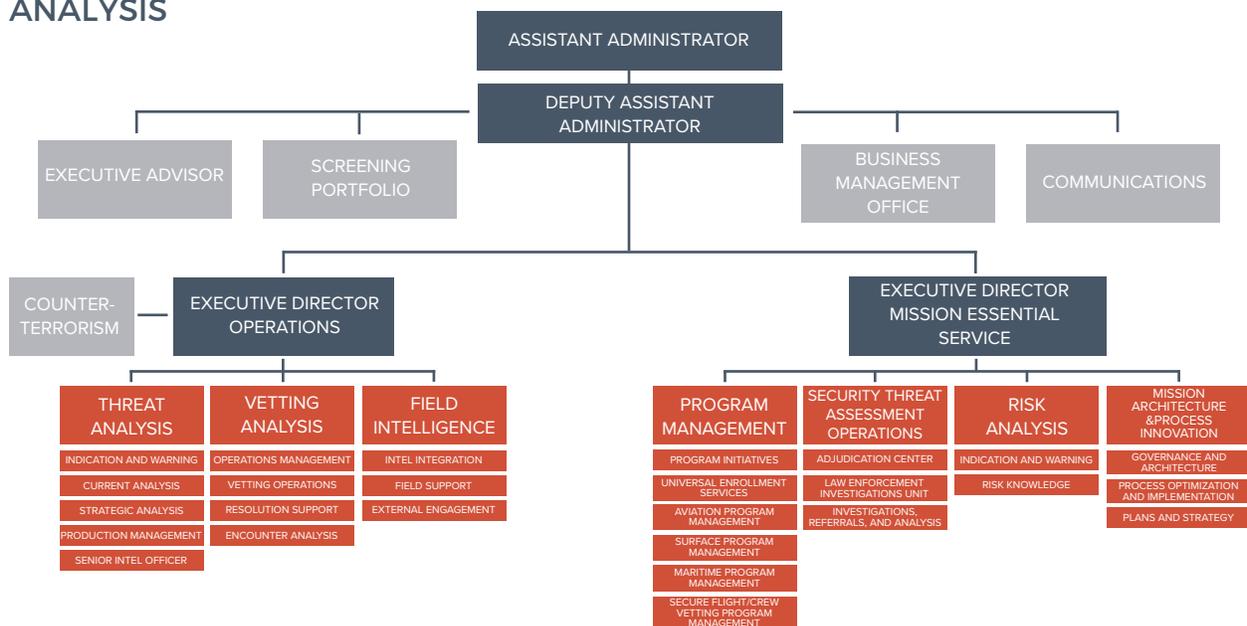
Source: Email from CBP Office of Legislative Affairs to Committee, July 14, 2016

CBP OI’s mission statement appropriately reflected its border security mission. As discussed previously, however, the ambiguity with regard to the total number and composition of its CIPs (in addition to OI) is confusing and makes coordinating the Component’s efforts difficult. CBP told the Committee that “[p]ersonnel supporting USBP intelligence analysis include 1024 Border Patrol Agents and an additional 222 [p]rofessional employees.”⁷⁸ This means that USBP intelligence activities – not part of CBP’s CIP – employ more than five times the number of FTEs than OI (237).⁷⁹ Although significantly smaller than USBP, CBP has two additional subordinate organizations conducting intelligence functions as well. OFO personnel at the NTC lead “operations that provide advance targeting, research, analysis, and coordination among numerous law enforcement and intelligence agencies in support of the CBP anti-terrorism mission.”⁸⁰ CBP OI told the Committee that it works with the NTC every day and has a “constant dialogue” with OFO personnel there. CBP OI also permanently stations five employees at the NTC.⁸¹ CBP’s AMO has an additional 28 GS-0132 employees facilitating the “coordination and interdiction of foreign and domestic threats posed by criminals, terrorists, and emerging security threats operating within and exploiting the air and maritime environments.”⁸²

Explaining this structure, CBP told the Committee that OFO, USBP, and AMO intelligence coordinate their activities with CBP OI representatives both at CBP headquarters and in the field. OI also provides collection plans to these organizations' intelligence elements. CBP officials described OI's role as providing more strategic analysis while the other CBP intelligence groups were more focused on more immediate, tactical needs.⁸³ Despite these explanations, the Committee views the fragmentation of CBP intelligence activities across the organization as not conducive to the best possible terrorism intelligence sharing efforts. As is clear in other parts of DHS, as well as other federal government agencies, creating separate structures within the same organization that conduct similar missions creates both overlap and stove-piping.

Recommendation: CBP should consolidate all of its intelligence functions under one CIP.

TRANSPORTATION SECURITY AGENCY, OFFICE OF INTELLIGENCE AND ANALYSIS

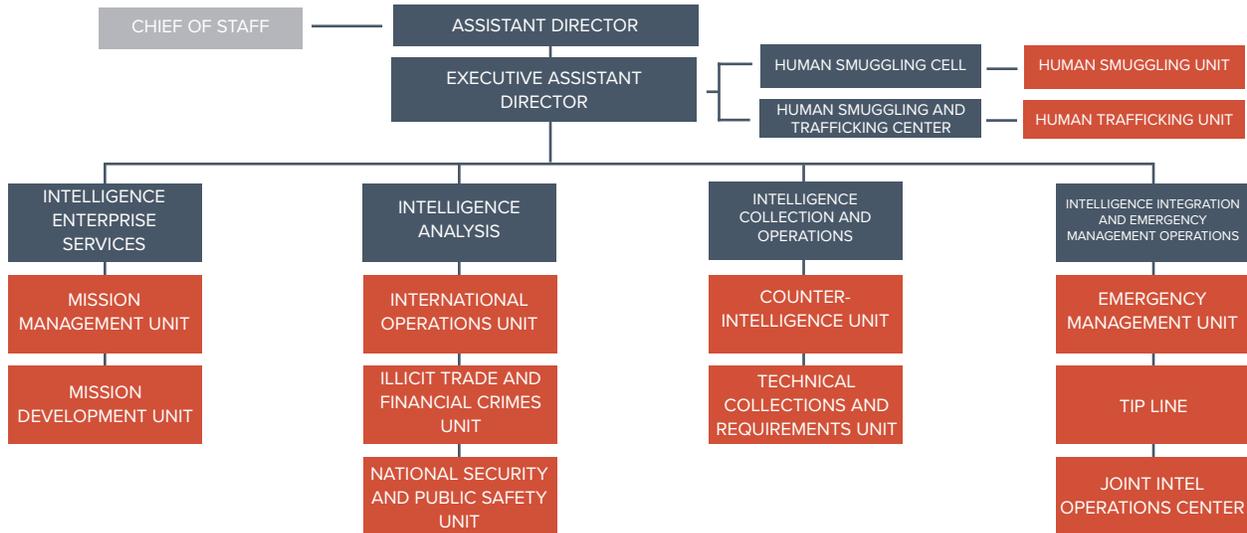


Source: Email from TSA Office of Legislative Affairs to Committee, July 14, 2016

TSA has historically been focused on transportation security intelligence.⁸⁴ TSA OIA's publicly posted mission statement, however, conflicts with what it provided to the Committee in its formal responses.⁸⁵ TSA OIA officials acknowledged their organization's evolving mission, and were conducting an in-depth mission analysis, as of early August 2016. OIA has created a Mission Architecture and Process Innovation (MAPI) office to spearhead this process, the end goal of which is to arrive at a five year strategic plan as well as a new mission statement.⁸⁶ This review process appears to have led to the designation of three CIPs *within* OIA: the Threat Analysis Division, the Field Intelligence Division, and the Encounter Analysis Branch in the Vetting Analysis Division.⁸⁷ In October 2016, the CINT Staff said that TSA "preferred not to identify all of OIA as a CIP due to the fact that there are many people in OIA who are not conducting intelligence activities."⁸⁸ As with CBP, this fragmentation creates the potential for uncoordinated and overlapping intelligence efforts.

Recommendation: TSA should consolidate all of its intelligence functions under one CIP.

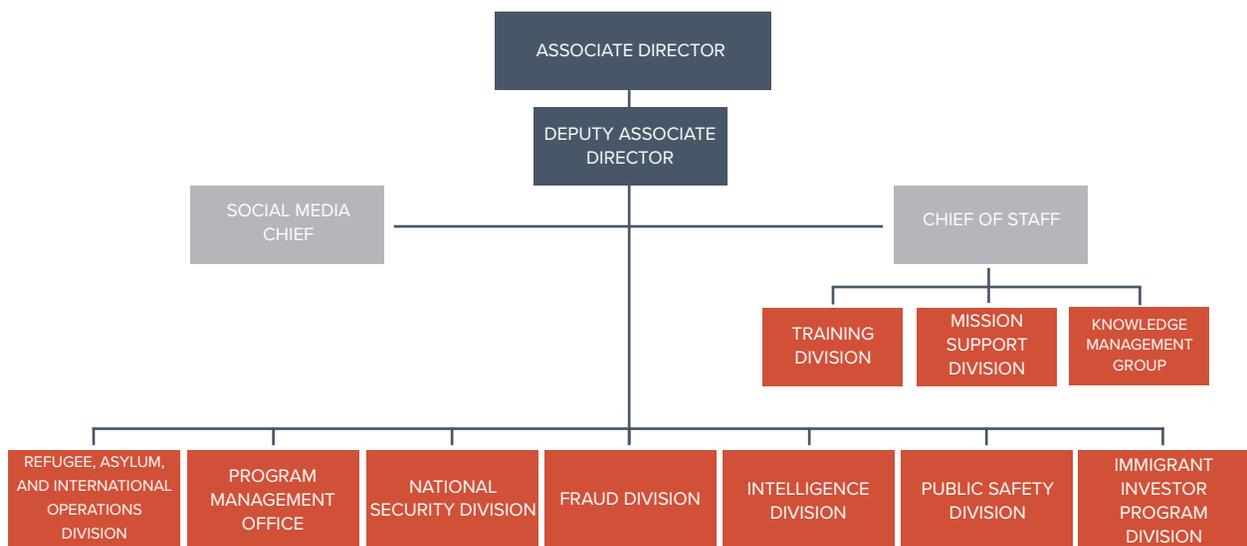
IMMIGRATION AND CUSTOMS ENFORCEMENT, HOMELAND SECURITY INVESTIGATIONS, OFFICE OF INTELLIGENCE



Source: Email from ICE Office of Congressional Relations to Committee, September 20, 2016

ICE’s HSI-Intel office has the best defined mission of any CIP the Committee reviewed. It addresses specific tasks for which the CIP is responsible, providing guidance to employees on exactly what is expected of them. One former DHS official the Committee interviewed described ICE’s intelligence organization as being well-structured for the organization’s analytical requirements.⁸⁹ Although not explicitly reflected in its mission statement, the ICE CIP conducts both case-support analysis and broader “strategic” analyses of relevant trends, according to another former DHS official.⁹⁰

UNITED STATES CITIZENSHIP AND IMMIGRATION SERVICES, FRAUD DETECTION AND NATIONAL SECURITY DIRECTORATE

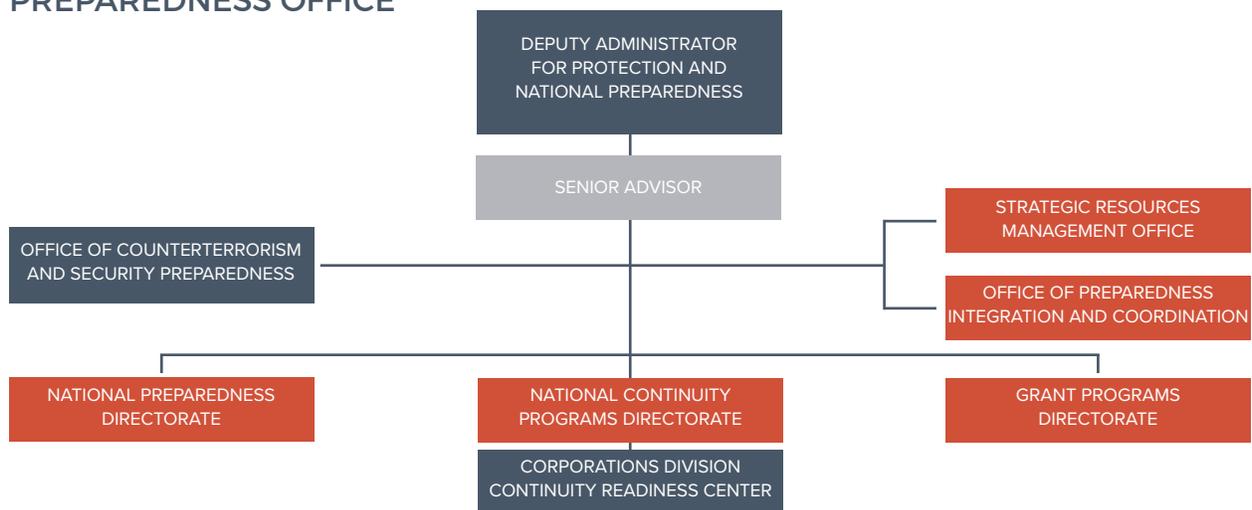


Source: Email from USCIS Office of Legislative Affairs to the Committee, June 21, 2016

USCIS' FDNS also has a tightly worded description of its intelligence activities, although, unlike ICE, it does not consolidate all of its intelligence activities under one CIP.⁹¹ As of October 2015 USCIS had designated two CIPs in addition to the Fraud Detection and National Security Directorate: the Collateral Duty Intelligence Officers of the Field Operations Directorate, and the Office of Security and Integrity of the Management Directorate. This separation gives the Committee cause for concern due to the possibility of overlapping and uncoordinated intelligence efforts. By unifying all foreign intelligence and counterintelligence efforts under a single CIP, USCIS would be better able to standardize procedures, report formats, and priorities.

Recommendation: USCIS should consolidate all of its intelligence functions under one CIP.

FEDERAL EMERGENCY MANAGEMENT AGENCY, PROTECTION AND NATIONAL PREPAREDNESS OFFICE



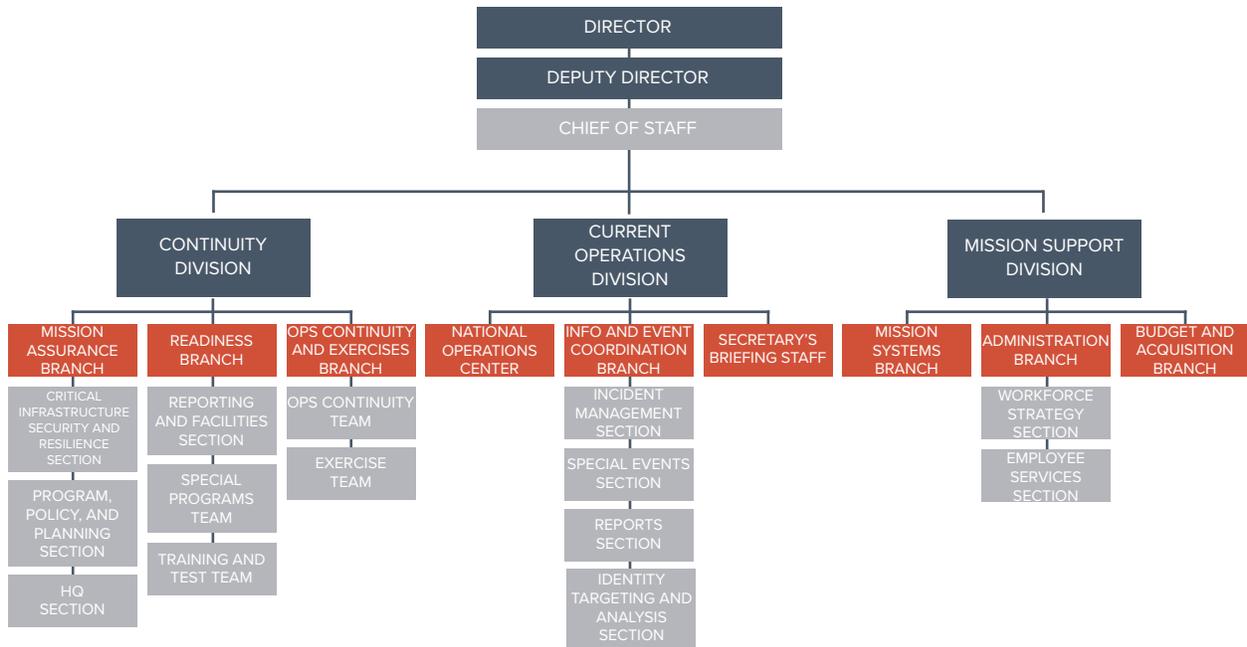
Source: Email from FEMA Office of Legislative Affairs to Committee, May 5, 2016

FEMA's CIP is its Protection and National Preparedness (PNP) office. The Committee is concerned with FEMA's perspective regarding its intelligence-related duties. FEMA told the Committee that "as a Non-Title 50 element, FEMA does not collect, analyze, or produce intelligence product[s]." This characterization also somewhat conflicts with the CIP's mission statement regarding its "development of threat assessments based on access to relevant IC and OPEN SOURCE reporting that inform the situational awareness and decision making of FEMA Senior Leadership."⁹² Furthermore, the agency went on to write that its PNP "is a consumer of Intelligence and uses this in conjunction with other information streams from a variety of sources to develop threat assessments that support the missions and operations of all FEMA elements and those entities to which FEMA provides support in the event of emergency or catastrophic events in an all-hazards context."⁹³ In the Committee's view, the aforementioned activities do constitute intelligence analysis.⁹⁴

Recommendation: FEMA should more clearly define its CIP mission statement.

Recommendation: The CINT should more closely examine the office's relationship with FEMA, and that organization's interaction with the broader IE.

OFFICE OF OPERATIONS COORDINATION AND PLANNING

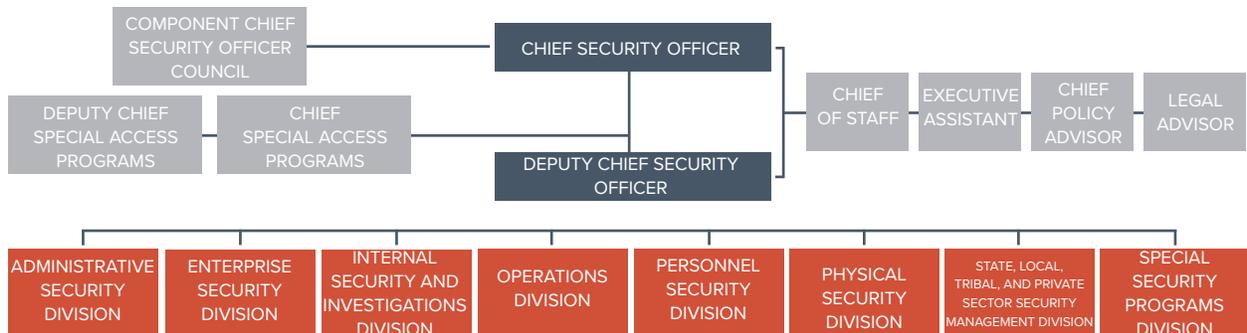


Source: Email from I&A Office of Legislative Affairs to Committee, April 28, 2016

Although not maintaining a formal CIP, OPS described its National Operations Center (NOC) “as the principal operations center for the Department” which provides “situational awareness and a common operating picture for the entire Federal Government” as well as SLTT authorities.⁹⁵ Despite not being a designated KIO, the OPS Director is a member of the HSIC.⁹⁶ Furthermore, OPS told the Committee that “as a member of the DHS IE and a customer of intelligence information, the office does have a close relationship with the DHS Chief Intelligence Officer.”⁹⁷ As is discussed later in this report, the Committee has found that DHS IE members – OPS among them – produce a significant amount of information of intelligence value that is not necessarily recorded, serialized, and disseminated.

Recommendation: The CINT should more thoroughly integrate OPS into the IE, especially with regard to dissemination of information of potential intelligence value derived from open sources and SLTT law enforcement organizations.

OFFICE OF THE CHIEF SECURITY OFFICER

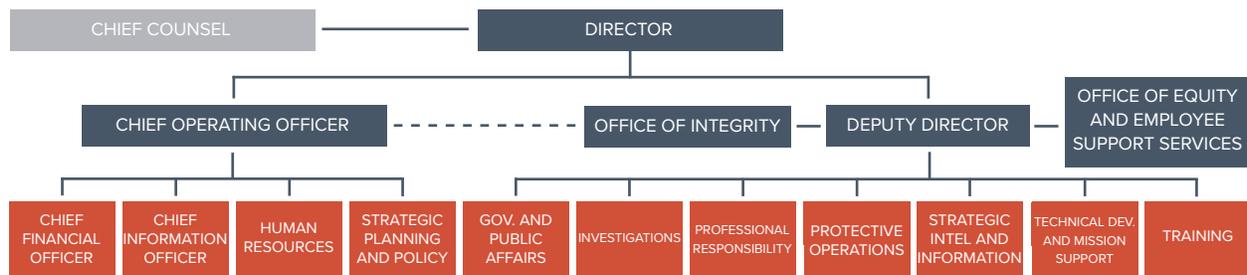


Source: Email from OCSO Office of Legislative Affairs to the Committee, May 9, 2016

OCSO told the Committee its mission was to ensure the “[p]rotection of personnel, information, facilities, property, equipment and other material resources.”⁹⁸ Although it does not maintain a CIP, the Committee believes that OCSO should play a role in helping to coordinate the Department’s intelligence activities and policies. A more tightly defined mission statement, specifically identifying how it interacts with the rest of the IE, would assist in this regard. The Committee will continue close oversight of OCSO to determine if substantive policy or legal changes are in order.

Recommendation: The OCSO should more clearly define its mission statement.

UNITED STATES SECRET SERVICE



Source: Email from I&A Office of Legislative Affairs to Committee, April 28, 2016

USSS maintains an Office of Strategic Intelligence and Information, headed by an Assistant Director who sits on the HSIC.⁹⁹ USSS employees also work with Intelligence Functional Managers (IFM) on the Analysis and Production and Collection and Reporting Boards.¹⁰⁰ As it does not have a CIP, the USSS declined to provide a mission for its intelligence office to the Committee.¹⁰¹ Overall, however the “Secret Service’s mission is two-fold: protection of the [P]resident, [V]ice [P]resident and others; and investigations into crimes against the financial infrastructure of the United States.”¹⁰² The USSS, with previously identified legislative and policy exceptions to its intelligence-related responsibilities, thus conducts its protective intelligence activities essentially separately from the CINT.¹⁰³ With a very narrow CT mission – specifically focused on its protectees – USSS intelligence as it relates to its protective mission is generally outside the scope of this report.

With regard to its investigative mission, Congress authorized the USSS to investigate violations related to credit card and computer fraud in 1984.¹⁰⁴ In 1990, it further authorized the USSS – in conjunction with the Department of Justice (DOJ) – to conduct civil or criminal investigations of federally insured financial institutions, including their electronic networks.¹⁰⁵ The USA PATRIOT Act of 2001 required the USSS to establish a nationwide network of Electronic Crimes Task Forces (ECTF) responsible for combatting a wide variety of cyber and electronic crimes.¹⁰⁶ According to the USSS web site, the organization’s “investigative mission abroad is growing as well, creating the need for a heightened overseas liaison presence.”¹⁰⁷ Although not necessarily directed towards CT, these investigative efforts can uncover information of intelligence value relevant to other topics. The extent to which USSS integrates its investigative efforts with the rest of the DHS IE thus warrants deeper investigation in the future.

VI. Intelligence Enterprise Information Sharing within the Federal Government

The Department collects a large amount of data of possible intelligence value and relevant to U.S. federal government CT efforts. The USCG Automatic Identification System (AIS), for example, is a maritime navigation safety communications system that tracks a vessel's characteristics including its type, position, course, speed, navigational status and other safety-related information.¹⁰⁸ Capable of handling over 4,500 reports per minute, the AIS updates as often as every two seconds while ensuring reliable ship-to-ship operation.¹⁰⁹ CBP's Advance Passenger Information System (APIS) allows DHS to review information – such as name and country of passport issuance – from every passenger boarding a commercial flight arriving into or departing from the United States.¹¹⁰ These two data sets highlight how DHS-derived information can potentially be a valuable source of intelligence. The Committee found that ensuring the IE is able to harness this wealth of information for intelligence purposes, however, has still proven difficult, even 15 years after 9/11.

POLICY ISSUES

Statutory and Policy Framework

The U/SIA has a variety of legal authorities and responsibilities with regard to information sharing with the federal government, vested both in statute and by delegation from the Secretary. One of these includes insuring “the timely and efficient access by the Department to all information necessary to discharge the [office’s] responsibilities including obtaining such information from other agencies of the Federal Government.”¹¹¹ The U/SIA also has statutory authority to access all U.S. federal government-derived intelligence – raw and finished – related to terrorism and infrastructure vulnerabilities.¹¹² Additionally, DHS policy also requires that Components “share information as one Department, rather than as separate entities to the extent permitted by and consistent with those Component Heads’ authorities and any restrictions imposed by statute, executive order, presidential or other directive, or national or departmental policy.”¹¹³ Finally, the CINT can establish “intelligence collection, processing, analysis, and dissemination priorities, policies, processes, standards, guidelines and procedures for the DHS Intelligence Components.”¹¹⁴

In addition to these legal and policy requirements, Congress has enacted additional incentives to share information. For example, agency heads “may consider the success of an employee in appropriately sharing information...including homeland security information, terrorism information, and weapons of mass destruction information, or national intelligence...in a manner consistent with any policies, guidelines, procedures, instructions, or standards established.”¹¹⁵ Law further requires that the U/SIA “evaluate how employees of the Office of Intelligence and Analysis and the intelligence Components of the Department are utilizing homeland security information or national intelligence, [and] sharing information within the Department.”¹¹⁶

Finally, DHS, the IC, and DOJ agreed in a separate 2003 memorandum to “establish procedures and mechanisms to provide DHS, and, as appropriate and practicable, other covered entities, with access to databases containing” terrorism and other DHS-relevant information.¹¹⁷ Furthermore, they concurred that “procedures and mechanisms for information sharing, use, and handling shall be interpreted and implemented consistently and reciprocally.”¹¹⁸

In spite of all these requirements, there remain significant cultural and policy impediments to CT information sharing within the DHS IE, and between it and the rest of the federal government. One former DHS official remarked that although the IT architecture necessary to ensure “optimal” sharing was still lacking throughout the IE, technological reasons were not the primary inhibitor of optimal intelligence flows. In fact, governance, policy, and privacy concerns most inhibited sharing, in his opinion.¹¹⁹ Many I&A analysts do not have experience in the various DHS Components, which leads to a lack of understanding regarding their legal authorities, collection capabilities, and resultant data sets, according to former DHS officials.¹²⁰ This unfamiliarity creates an “unhealthy disconnect” between I&A’s intelligence mission and the law enforcement information that the Components collect under a variety of legal authorities.¹²¹

One way to help fix this disconnect would be standardizing and encouraging intelligence rotational programs. DHS IE employees are currently able to participate in three separate programs. The IC Joint Duty Program is one such program, open to members of IC agencies, the purpose of which is to “encourage and facilitate assignments and details of personnel to national intelligence centers and between elements of the intelligence community.”¹²² The Homeland Security Rotation Program (HSRP) is specific to the Department but not the DHS IE.¹²³ It “provides developmental assignments that give additional opportunities for employees to broaden their skills, gain organizational knowledge, and enhance their personal and professional growth.”¹²⁴ Finally, the Intelligence Rotational Assignment Program (IRAP) serves to “promote a broader understanding of the various intelligence missions and functions across the DHS IE and Fusion Centers” and “to enhance the career development of federal DHS Intelligence personnel through exposure to other DHS Intelligence Components and fusion centers.”¹²⁵

CINT staff members told the Committee that they tracked all DHS personnel rotations into and out of the IC, but there is less clarity with regard to how effectively IE organizations track HSRP and IRAP rotations.¹²⁶ This compounds what the Committee learned from the components; that there exist varying policies for how to monitor these assignments and take advantage of the experiences of personnel who have recently returned from rotations.¹²⁷

Recommendation: The CINT should conduct a detailed review of all intelligence rotational programs for which IE employees are eligible, standardizing, consolidating, and tracking the various programs to the greatest extent feasible.

Importance of Personal over Institutional Relationships

Former U/SIA Caryn Wagner described much of the work of the DHS IE as being based on personality, rather than an institutional framework.¹²⁸ At the more junior levels, personal relationships were the most important factor in determining whether a CIP would share intelligence, especially if derived from a sensitive source such as a case file, according to another former DHS IE official.¹²⁹ One knowledgeable person commented that, in terms of information sharing in the DHS IE, “everything is dependent on personal relationships.”¹³⁰ As a result, the person told the Committee that “one hand doesn’t know what the other is doing.”¹³¹ ICE’s KIO conceded to the Committee that intelligence sharing throughout the IE was “very personality-driven, unfortunately.”¹³² OPS employees described their relationship with both other federal agencies as well as SLTT law enforcement authorities as a “coalition of the willing...sometimes the unwilling.”¹³³

“One hand doesn’t know what the other is doing.”

AN OUTSIDE OBSERVE DESCRIBING THE INTELLIGENCE ENTERPRISE’S LACK OF COORDINATION

June 2016

Although the Committee understands the vital importance of professional relationships in ensuring the smooth flow of intelligence within the DHS IE, as well as with external federal stakeholders, these relationships appear to be the “glue” that holds the system together. A reliance on implicit understandings and culturally-ingrained ways of doing business are prone to failure when key individuals change positions or offices undergo reorganization. The optimal model would be one of “personally-mediated institutional frameworks,” whereby strong ties of trust between DHS personnel and their partners would facilitate rapid sharing of terrorism-related intelligence. In cases where these ties do not exist or become degraded, however, a clear institutional framework is necessary to serve as a backstop. By increasing the oversight of the CINT with regard to intelligence-sharing mechanisms and procedures, the DHS IE can more effectively ensure such arrangements survive the departure of key personnel or re-arranging of bureaucratic structures.

Managing Memoranda of Understanding

The CINT, via the statutory authority delegated by the Secretary, is authorized to “enter into cooperative arrangements with other executive agencies to provide such material or provide Department officials with access to it on a regular or routine basis, including requests or arrangements involving broad categories of material, access to electronic databases, or both.”¹³⁴ The Secretary has not further delegated this authority, however, beyond the U/SIA. The CINT also has the authority to “review, coordinate, and approve agreements between Components and elements of the IC before their execution in addition to overseeing the execution of those agreements,” except USSS protective intelligence agreements, according to DHS policy.¹³⁵ The Department’s policy also requires

that “prior to signing any MOU or MOA [Memorandum of Agreement], the person signing for DHS must ensure that Office of General Counsel has reviewed the document for legal sufficiency and approved it.”¹³⁶

There is unanimous agreement throughout the DHS IE that review of MOUs takes significant time and effort. It appears, however, that despite this long process, the CINT is not fully included in the approval and tracking of these agreements. At least from 2010 to 2012, the CINT had a database of all known DHS Component MOUs involving intelligence sharing between the Department and external organizations, according to one former U/SIA.¹³⁷ A former Congressional staff member with oversight responsibilities for DHS concurred that the CINT did track such MOUs as of 2012.¹³⁸ CINT Staff, however, told the Committee in early 2016 that they had no such compilation, although clarified later in the year that they had been tracking these agreements since 2007, but just did not have a complete list.¹³⁹ That the CINT does not have full visibility with regard to what intelligence the Department is sharing externally, which appears to be the case, is not in line with the aforementioned DHS policy that the CINT “review, coordinate, and approve” intelligence sharing agreements.

The Committee’s review of CIP practices similarly found significant disparity in terms of their coordination and cooperation with the CINT. CINT Staff members expressed special frustration with one Component in this regard, as that organization frequently would sign intelligence-sharing MOUs with outside agencies without notifying the CINT.¹⁴⁰ This same Component told the Committee – incorrectly – that under current policy, the CINT does not need to approve intelligence-sharing agreements with organizations outside of DHS.¹⁴¹ Its officials did, however, say that they would notify him upon signing such agreements, contradicting the CINT Staff’s complaints.¹⁴² Another component, conversely, told the Committee that it coordinates all information sharing MOUs with the CINT Staff.¹⁴³ Oddly, a third CIP told the Committee that it used DOJ standard formats for its MOUs.¹⁴⁴ Regarding these agreements, this same CIP wrote that it did not coordinate them with the CINT because “Federal Laws preclude these LE specific functions and actions [being] shared with a Title 50 agency [sic].”¹⁴⁵ Upon a request for elaboration from the Committee, officials from this CIP clarified that they did in fact coordinate such agreements, such as their intelligence sharing arrangements with local FBI Joint Terrorism Task Forces (JTTF) as well as the National JTTF, via the CINT.¹⁴⁶ Despite this clarification, it appears that some DHS CIP employees are reticent to coordinate intelligence-sharing agreements with the CINT. Such attitudes are also reminiscent of the pre-9/11 “wall” between law enforcement and intelligence functions, one of the many structural problems that led to the disaster.¹⁴⁷

Recommendation: The CINT, with the support of the Secretary, should more aggressively enforce the mandate to coordinate and approve all MOUs, and maintain an up-to-date list of all relevant intelligence-sharing agreements.

Raw Intelligence Reporting Formats

Following the tragic death of Central Intelligence Agency (CIA) officers in Khost, Afghanistan in 2009 at the hands of a suicide bomber whom the agency had up to that point been handling as an intelligence asset, the CIA conducted an in-depth review.¹⁴⁸ The review

task force's first publicly-available recommendation was to ensure "greater discipline in communications, ensuring that key guidance, operational facts, and judgments are conveyed and clearly flagged in formal channels."¹⁴⁹ If one agency faced such challenges, it is no surprise that an amalgamation of 22 previously independent organizations have experienced similar problems.

Capturing the information of intelligence value that the Department collects, and presenting it in a useable format, is a critical task for the DHS IE. U/SIA Taylor and his staff have pushed to develop standardized procedures for doing so, but much work remains. CINT Staff members acknowledged to the Committee that there were likely large quantities of documents generated by the DHS IE with potential intelligence value not captured in serialized reporting.¹⁵⁰ CBP's data sets have been especially challenging to integrate into the DHS IE's efforts, according to one observer.¹⁵¹ The fact that nearly one million people legally enter the borders of the United States every day, through a variety of methods and ports of entry, is a major contributing reason.¹⁵² Ensuring that such valuable information finds its way to the correct analysts is a vital but challenging task, according to another.¹⁵³ Indeed, I&A writes approximately 5% of CIP Intelligence Information Reports (IIR) due to their low number of reports officers, and then sends the documents back to the Components for issuance.¹⁵⁴ That some CIPs require I&A's help to turn raw information into intelligence reporting suggests there is even more Component information never reported in formal channels.

The infrastructure for reporting this information already exists to some degree in the DHS IE. The Human Intelligence (HUMINT) Online Tasking and Reporting (HOTR) platform is the Enterprise's standard raw intelligence reporting system. HOTR allows the drafting of IIRs for dissemination to all cleared personnel with a need-to-know.¹⁵⁵ Although HOTR and the IIR format have been in use for quite some time, the CINT finalized a unified IIR policy only in August 2016; the policy was still under Office of General Counsel (OGC) review as of November.¹⁵⁶ The Department also established a Reports Officer Management Council (ROMC) – recently renamed the Human Derived Intelligence Working Group – to manage this and other policies related to raw intelligence reporting.¹⁵⁷ DHS personnel are also auditing an FBI "release authority" course to determine how best to structure the Department's own course supporting this requirement.¹⁵⁸ Ongoing efforts to standardize intelligence reporting throughout the IE are appropriate and necessary.

DHS CIPs have embraced such standardization efforts to varying degrees. CBP told the Committee that it backed CINT efforts to standardize IIR procedures, and thought the efforts of the ROMC were useful.¹⁵⁹ This is understandable, because until early 2016, CBP did not have release authority for IIRs, having to route them to I&A for review. As with MOUs, the Committee believes that the CINT should review intelligence sharing procedures such as IIR dissemination. Once established, however, the CIPs should be able to execute these processes without further CINT approval (although still notifying him). Allowing CBP to release reports directly allows for greater speed and availability of information, highlighted by the fact that CBP increased its IIR production by 114% following this policy change.¹⁶⁰

Despite its enthusiasm for standardizing the IE IIR process, however, CBP continues to experience challenges with regard to disseminating raw information of intelligence value. Documenting key meetings, international engagements, directives, and other occurrences is difficult, due to lack of any systematic methodology for doing so, according to one observer.¹⁶¹ Exacerbating the problem, CBP also maintains two distinct raw reporting vehicles: Field Intelligence Reports (FIR) and IIRs.¹⁶² CBP maintains FIRs for internal use only in its Intelligence Reporting System (IRS) database, although some ICE personnel also have access. When information meets national intelligence requirements, CBP will issue an IIR for the entire IC.¹⁶³ USCG-Intel also writes FIRs for use within the organization only, although this system is separate from CBP's.¹⁶⁴ CINT Staff members were generally impressed with USCG's FIR process, and were seeking to employ some of the Coast Guard's best practices throughout the DHS IE.¹⁶⁵ The fact that DHS CIPs retain information of intelligence value, without making it discoverable to other organizations with a need-to-know, however, requires further examination.

Although CBP and USCG appear to be seeking to document their vast data holdings in a more standardized format and allow their discoverability outside the organization, ICE told the Committee that it intentionally limits the distribution of many of its intelligence products.¹⁶⁶ This desire has the potential for negative consequences to CT and other DHS efforts. Incompatibility and lack of intelligence sharing between ICE and USCIS systems has, for example, prevented easy identification of human traffickers, according to a 2016 DHS OIG report.¹⁶⁷ The DHS OIG found that "opportunities existed for improved data exchange between ICE and USCIS," because "ICE did not always advise USCIS of the victims they identified in the course of human trafficking investigations," nor did ICE "always consult with USCIS to determine if traffickers, particularly employers, brought other potential victims into the United States."¹⁶⁸ The Committee recognizes that this lack of sharing was two-way, as USCIS employees did not routinely share with ICE the data they collected on potential human traffickers.¹⁶⁹ There is significant evidence of terrorists funding and facilitating their operations via human trafficking, highlighting the importance of remedying the aforementioned barriers to information sharing.¹⁷⁰

Such attitudes with respect to sharing information in human trafficking also highlights the potential for unnecessary obstacles in CT investigations. One CINT Staff member likened ICE's behavior with regard to UNCLASSIFIED information to treating it "as a SAP [Special Access Program]," when the situation did not warrant doing so.¹⁷¹ Although hyperbole, this statement does highlight a trend the Committee has also detected with regard to ICE's CIP. Discussing these issues with the Committee, ICE HSI-Intel officials expressed frustration that outside organizations frequently requested access to large quantities of their data. As much of ICE's information is UNCLASSIFIED, these outside groups – whether other DHS CIPs or in the IC – did not demonstrate consistent commitment to protecting said data. Despite its lack of classification, ICE HSI-Intel contested, much of this information indeed required strong protections.¹⁷² This CIP often keeps sensitive operational information – such as that related to confidential informants, search warrants, and enforcement actions – intermixed with other, more mundane information. Sifting through these data in response to external requests takes significant amounts of its employees time.¹⁷³ ICE in fact maintains a relatively robust cadre of reports officers to conduct these tasks.¹⁷⁴ ICE HSI-Intelligence anticipated

that the Data Framework (discussed in detail later) would ameliorate the aforementioned problems. By automating the categorization of data sets, ICE could release intelligence information while preventing the disclosure of sensitive operational data.¹⁷⁵

Recommendation: The CINT should standardize raw intelligence reporting formats throughout the Department and create a system of record for dissemination, discoverable by all personnel with a need-to-know, even for products containing information that does not meet the standard for national intelligence reporting.

Recommendation: The CINT should ensure these raw intelligence reporting formats allow for segregation of sensitive data from less critical information, and ensure said formats are compatible with and easy to manipulate via the DHS Data Framework.

In addition to information derived from operational and law enforcement activities, the DHS IE draws a large amount of information from open sources. These efforts appear piecemeal and uncoordinated. When asked about its efforts to coordinate its open source reporting with I&A and the Office of the DNI's (ODNI) Open Source Center (OSC), one Component told the Committee that de-conflicting with "[O]DNI and I&A open source capabilities is not necessary."¹⁷⁶ When discussing this same issue with the CINT staff, they similarly dismissed the need to coordinate IE open source intelligence efforts with the ODNI OSC, citing the fact that DHS' mission primarily focused on domestic issues while the OSC concentrated its intelligence collection abroad.¹⁷⁷ In its review of intelligence products from all DHS IE members, however, the Committee found that a majority included at least some open source information regarding overseas events and threats. By taking advantage of readily-available IC initiatives and better focusing its collection efforts on domestic topics, the DHS IE could likely prevent duplication, save money, and use its employees time more efficiently.

The Committee identified uncoordinated analysis of publicly available information in several DHS Components. As previously discussed, CBP creates FIRs, which may contain open source reporting, but usually only disseminates them internally.¹⁷⁸ TSA uses commercial data mining services to identify relevant events.¹⁷⁹ To monitor breaking media developments, OPS maintains a contract with a private company that employs two full-time analysts who monitor open source outlets for breaking news. One analyst views "traditional media" such as cable television news while the other monitors "non-traditional media" such as social media networks. OPS employees told the Committee that they receive 94% of their situational awareness cueing from this source.¹⁸⁰ OPS' relatively labor-intensive method of monitoring open source information sources stands in stark contrast to the automated systems which other Components such as TSA employ. This wide variety of different methods for gleaning information of intelligence value from publicly available information is less than optimally efficient and potentially duplicative.

The CINT Staff, as well as DHS officials who testified before the Committee previously, have drawn a stark distinction between "media monitoring" and open source intelligence collection.¹⁸¹ The Committee understands the difference established in DHS policy between the two, specifically with regard to the collection of Personally Identifiable Information (PII),

but does not view them as mutually exclusive activities. By ensuring information gleaned from publicly available sources is discoverable by all DHS personnel with a need-to-know, regardless of method of collection, the Department could streamline its efforts to capture this information and save taxpayer dollars. The DHS CIPs also automate their open source data mining efforts to varying degrees. Standardizing and consolidating these efforts would both save money and make IE open source analysis more effective

Recommendation: The CINT should use existing legal authorities to standardize methods for collecting open source information and disseminating reporting derived from it throughout the IE.

Recommendation: The CINT should review existing IC open source collection and analysis capabilities and determine whether the DHS IE can use some of these resources instead of pursuing similar initiatives “in-house.”

Finished Intelligence Products

The CINT, in some cases via delegation from the Secretary of Homeland Security, has the statutory authority and responsibility to “integrate the information and standardize the format of the products of the intelligence Components of the Department containing homeland security information, terrorism information, weapons of mass destruction information, or national intelligence.”¹⁸² A member of the CINT Staff acknowledged this authority, but told the Committee that the CINT simply had not yet exercised it.¹⁸³ There is a clear, pressing need to do so. A Committee review of DHS-provided products revealed 56 different finished intelligence formats; almost every CIP had at least one unique product type. Understanding these circumstances, and in an effort to quantify the finished analysis the Department produces, the CINT Staff has created a “Homeland Intelligence Product Repository.” In April 2016, the CINT issued a directive to the IE requiring that all CIPs submit their finished intelligence products to a centralized repository.¹⁸⁴ The task of merely putting information into these various formats is an enormous drain on analyst resources. Furthermore, it confuses readers who might not instinctively understand the scope, sources, and purpose of each document. Consolidation of these disparate product types throughout the IE would save time for both intelligence producers and consumers.

Recommendation: The CINT should standardize all DHS IE analytical product formats where practicable.

Recommendation: DHS Components should produce the minimum number of different formats of finished intelligence as is necessary.

“[E]ffective analysis requires blending together information both from traditional intelligence community sources” as well as from law enforcement and other authorities, according to one former DHS IE official.¹⁸⁵ The DHS IE, however, frequently repackages analysis from other organizations into its finished intelligence products. Although the Committee understands that the intent of some of these product is to provide IC-derived analysis to SLTT and other relevant law enforcement organizations, there are more effective ways to

do so. The CINT, on behalf of these stakeholders and representing the entire IE, should work with the IC to ensure that the necessary products are discoverable to those with a need-to-know, rather than converting them into DHS-branded products.

The Committee reviewed I&A's "Homeland Intelligence Daily" for approximately two months, and found that it frequently copied analytical products from IC agencies and organizations and simply re-published them one or more days later. TSA's "Daily Stakeholder Information Report" similarly seems to be generally a repackaging of IC information into a TSA document.¹⁸⁶ Furthermore, TSA told the Committee that "about 99 percent of classified information in our products is from the IC," that it "most often produce[s] finished intelligence products derive[d] from IC raw intelligence reporting," and "routinely creates Intelligence Notes completely absent of information from DHS Components."¹⁸⁷ In the view of the Committee, TSA OIA's most useful products were IIRs and Transportation Suspicious Incident Reports (TSIR) derived from TSA operations, a unique source of information to which no one else in the IE or IC would have access. Focusing on products such as these, rather than recreating IC analyses, would better serve all stakeholders. The aforementioned former DHS official told the Committee that, based on his recent discussions with SLTT law enforcement organizations, I&A in particular was in fact moving in the opposite direction: focusing more on creating products similar to those from the IC. This was to the detriment of intelligence efforts that capitalized on the data sets unique to DHS, in his view.¹⁸⁸

Recommendation: The CINT should ensure that all appropriately cleared SLTT officials with a need-to-know can access relevant IC-created intelligence products to the extent practicable, rather than repackaging these products and disseminating them directly.

In addition to its raw reporting derived from publically available information, the Committee has found in some instances that DHS CIPs have produced finished intelligence products of questionable value using open source information. OCIA-ISB sent the Committee an "Inspire Magazine Sector Threat Focus" product which pulled exclusively from open source information, and is very similar to analyses such as those produced by private organizations, which publish their products far more rapidly.¹⁸⁹ Especially interesting to the Committee was the fact that FPS's TMD created a product that cited the Committee's monthly Terror Threat Snapshot product line.¹⁹⁰ The fact that FPS hires contractors to create products for its senior leadership, using its oversight Committee as the source of information, is not an effective use of taxpayer dollars. FPS-TMD uses the same contract as DHS I&A to hire contract analysts for its production requirements, which is reflected in the similar characteristics of I&A open source products identified during the Committee's review.¹⁹¹

Recommendation: The CINT should conduct an audit of all contractors conducting open source analysis throughout the DHS IE, and consolidate their efforts as much as possible.

Recommendation: CIPs should buy commercial subscriptions for open source analysis when appropriate, rather than hiring contractors to produce similar material.

Focusing on I&A specifically, one outside group has suggested that this CIP concentrate its analysis on the "aggregation of intelligence information from DHS subcomponent

agencies.”¹⁹² U/SIA Taylor told the Committee that he similarly believes I&A should focus its efforts on DHS-unique information.¹⁹³ I&A has thus designed performance metrics to encourage the use of DHS Components, SLTT, private sector, and open source information. In Fiscal Year (FY) 2016, I&A intended to use such information in 80% of its products.¹⁹⁴ Although I&A is taking steps to focus its efforts on DHS-derived information, the Committee does not sense other CIPs share this sentiment. One former official told the Committee that “DHS analyst[s] have been uncomfortable looking beyond traditional IC” reporting in their work.¹⁹⁵ By evaluating non-traditional information, however, is how the DHS IE can make its greatest contribution to our nation’s security.

Recommendation: The CINT should develop a plan to incentivize and evaluate the use of DHS-derived information in the analytical products of all IE members as appropriate.

Discoverability

Ensuring the formal documentation of information of intelligence value is an important way to ensure that all relevant stakeholders can access it. An effective method for storing and disseminating these data is equally critical. A key distinction among information sharing efforts and systems is whether they automatically make data available to other organizations or share only by request.¹⁹⁶ The ability to conduct “self-service” is extremely important for analysts. The time, resource, and bureaucratic costs of specifically requesting information from other organizations serve as strong impediments to actually making such requests. Especially with regard to terrorist threats to the Homeland, incentivizing such transfer of intelligence through effective systems architecture is a critical, if not overdue, task.

Perhaps the best indicator of the “discoverability” of intelligence is the manner in which potential customers learn of its existence. Throughout the DHS IE, manual methods appear to be commonplace, indicating a lack of ability to access key data by default. USCG-Intel often notifies known customers of recently completed products via e-mail and/or phone call to cue them to log in to their classified systems.¹⁹⁷ CBP primarily alerts customers to the publication of finished intelligence via e-mail.¹⁹⁸ TSA appears to rely heavily on phone calls and e-mails to notify customers of the issuance of analytical products.¹⁹⁹ OPS provides much of its reporting via e-mail, although partner organizations also regularly view the DHS Common Operating Picture (COP).²⁰⁰ Even though ensuring receipt of critical intelligence via phone or e-mail can serve as an important failsafe measure in time-sensitive scenarios, it in fact appears to be the primary method of notification in the DHS IE. Automating these processes and using manual means as a last resort could help improve the Department’s analytical efficiency and effectiveness.

An anecdote from another organization is useful in highlighting the perils of this method of intelligence sharing. One 15-year CIA veteran, reflecting on his time at the agency’s Counterterrorism Center immediately after 9/11, said “I don’t want to exaggerate but I think we might have gotten a thousand emails a day. And if a crisis hits, the same thing could happen again easily, because people will send everything to everybody out of self-defense, even though that itself creates a problem.” He continued, saying that “as a consequence of too much information sharing, key pieces of information sharing may be ignored. And they

might have gone ignored in the days after 9/11 when we got a thousand emails a day.”²⁰¹

Although not applicable to most of the DHS IE, Intelligence Community Directive (ICD) 501 provides a policy framework for addressing such problems. Issued in 2009, this ICD assigns IC personnel a “responsibility to discover” information that they believe to have the potential to contribute to their assigned mission need.²⁰² Furthermore, it assigns the stewards of data a “responsibility to provide” by making “all information collected and all analysis produced by an IC element available for discovery by automated means by authorized IC personnel.”²⁰³ Such a policy requires making information of potential intelligence value available to everyone with a need-to-know, with some exceptions in the case of sensitive sources or methods.²⁰⁴ Rather than sorting through e-mails and other documents for desired pieces of information, analysts can query databases for only the data they require. The DHS IE, with its vast repositories of data, would be able to execute its CT intelligence function more effectively with guidance similar to that which ICD 501 provides.

Recommendation: The CINT should issue an intelligence “discoverability” directive similar to ICD 501.

Towards a Departmental Intelligence Doctrine

One former CINT told the Committee that it was often unclear as to who has the responsibility and/or ability to compel information sharing, owing to the lack of a Departmental intelligence doctrine. Even when policy was explicit, practice often differed from it, especially with regard to restricted or sensitive information, such as investigative case files or highly classified IC material. He thus recommended creating a “compulsory methodology” for intelligence sharing.²⁰⁵ During her 2011 testimony before the Committee, former U/SIA Wagner stated that the Department was exploring the feasibility of a Departmental intelligence doctrine.²⁰⁶ As of August 2016, no such unifying doctrine existed, although the need for it is clearly evident.

A perfect example of DHS’ lack of consistent doctrine with regard to the IE is a document that TSA’s OIA produced. Entitled “Differences between Information and Intelligence,” this article and graphic (apparently a “Transportation Intelligence Note” despite not mentioning any transportation security issues) defines intelligence in terms of DoD manuals and information posted to the FBI’s public web site.²⁰⁷ The fact that one CIP has created its own definition of intelligence, different than that enshrined in DHS policy, reveals how achieving consensus on the most basic issues is difficult without a Department-wide doctrine.²⁰⁸

Recommendation: The CINT should develop and issue a Departmental Intelligence Doctrine, using relevant Component policies and IC Directives as a starting point.

TECHNOLOGY ISSUES

Although the Department has made great strides towards ensuring the interoperability of its various information systems, significant room for improvement remains. The U/SIA is responsible for ensuring “that any information databases and analytical tools developed or utilized by the Department...are compatible with one another and with relevant information databases of other agencies of the Federal Government.”²⁰⁹ Congress also required that DHS standardize “the information and data collected from foreign nationals, and the procedures utilized to collect such data, to ensure that the information is consistent and valuable to officials accessing that data across multiple agencies.”²¹⁰ In addition to the legal requirements placed on them, DHS, the IC, and federal law enforcement agencies agreed in a separate 2003 memorandum that the databases each of them used “should facilitate, to the greatest possible extent: ease and speed of information exchange; differentiated access [based on security clearance and need-to-know]...; and compatibility with other databases of” the parties to the agreement.²¹¹ Within DHS, policy requires that, to “the greatest extent feasible, Components standardize the technology used to categorize, access, exchange, and manage information in automated systems to permit the effective location and use of the most current and complete data available.”²¹²

A Multiplicity of Systems

Despite the aforementioned statutory and policy requirements, the Department currently does not currently satisfy them. Former U/SIA Caryn Wagner identified one of her major challenges as dealing with “legacy systems” containing “a great deal of data – travel data, immigration data, cyber data,” and that a “lot of that data is resident in different little stovepipes.”²¹³ CINT Staff members expressed to the Committee a strong desire to standardize the formats of intelligence databases resident within DHS Components.²¹⁴ The Department has approximately 900 different “structured databases,” located primarily on unclassified networks. Furthermore, of these, 250 have multiple data formats and standards, according to DHS documentation.²¹⁵ Specifically with regard to intelligence, the Committee identified 75 intelligence-specific databases of all levels of classification in use throughout the DHS IE (see Appendix I for details). The Department had previously explored creating an IE “Intelligence Suite” of default tools and databases for analysts, based on Component, according to a TSA OIA official. This effort, which spanned 2009-2010, however, appears to have been abandoned.²¹⁶

Many of the information systems on which these databases reside are outdated and insecure.²¹⁷ 203 sensitive but unclassified (SBU) and 17 SECRET or TOP SECRET of the Department’s systems were running without the required “authority to operate” (ATO), according to 2016 DHS OIG report. “Without ATOs, DHS cannot ensure that its systems are properly secured to protect sensitive information stored and processed in them,” according to the same report.²¹⁸ Although certain DHS efforts – such as conducting “Mission Support Review[s]” to assess the effectiveness and efficiency of efforts to deliver IT support – are positive steps, the Department needs to significantly overhaul its information systems.²¹⁹

“A lot of that data is resident in different little stovepipes.”

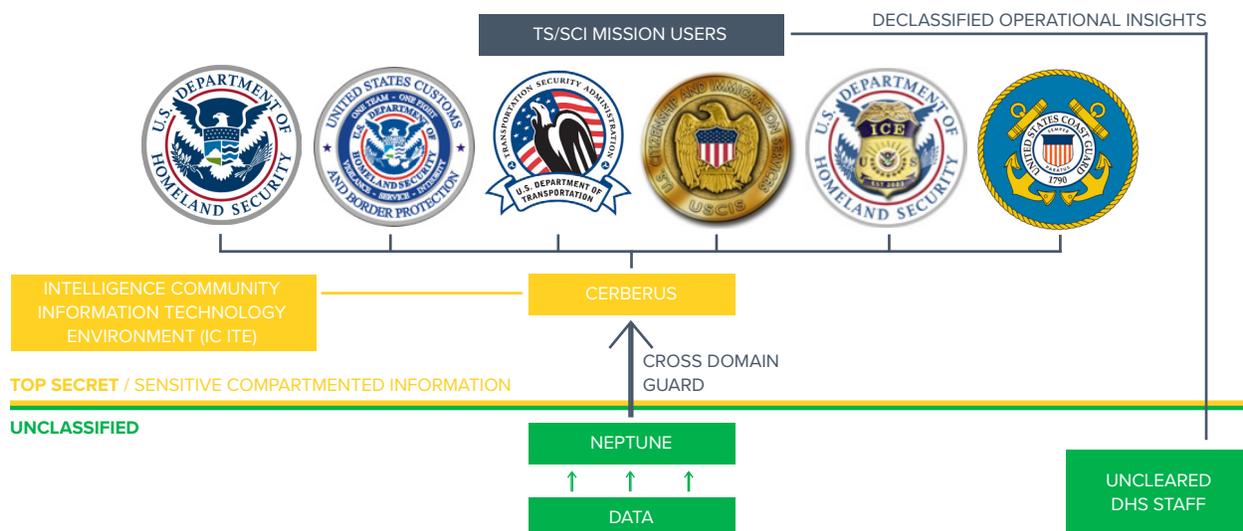
**CARYN WAGNER, THEN-UNDER SECRETARY
OFFICE OF INTELLIGENCE AND ANALYSIS
ON DHS DATA SYSTEMS**

June 1, 2011

The Data Framework

In an effort to harness the information of intelligence value that DHS collects, the Department is creating a “Data Framework” to manage its most important data sets of potential intelligence value. In conjunction with the DHS Chief Information Officer (CIO), the CINT is responsible for establishing “a comprehensive information technology network architecture for the Office of Intelligence and Analysis that connects the various databases and related information technology” for I&A and the CIPs “in order to promote internal information sharing among the intelligence and other personnel of the Department.”²²⁰ Thus, the legal and policy foundations for creating such a system already exist. U/SIA Taylor views standardizing IT architecture across Components as one of the areas in which the CINT can add the most value to the IE, and the Committee is in strong agreement with him in this regard.²²¹

The Data Framework comprises three subordinate systems: Neptune (SBU), Common Entity Index (SBU), and Cerberus (TOP SECRET/Sensitive Compartmented Information [TS/SCI]).²²² The purpose of the Data Framework system is to allow seamless access to vast number of different databases, based on mission needs and user clearance level, as well as to facilitate classified searches of unclassified data. The Department is building Cerberus in accordance with Intelligence Community Information Technology Enterprise (IC ITE) standards, which will allow enhanced sharing and security between DHS IE members and the IC.²²³ Although DHS plans to include 20 data sets by the end of 2016, only seven were currently capable of real-time transfer with the Data Framework as of November.²²⁴



Many DHS CIPs are actively embracing the DHS Data Framework, which the Committee views as a critical priority in exploiting the Department's vast information holdings. I&A is leading the initiative, and had nine personnel actively using the system as of early June 2016.²²⁵ USCG-Intel has incorporated its Ship Arrival Notification System (SANS) into the system and is actively developing an interface to access the Data Framework.²²⁶ CBP officials were similarly optimistic about the system when briefing the Committee, although mentioned that only TS/SCI-cleared personnel using the Cerberus module of the system had access as of early August 2016.²²⁷ U/SIA Taylor concurred that CBP was enthusiastically embracing the Data Framework project.²²⁸ TSA OIA officials were sanguine about the initiative, but indicated that automating the ingest of even the "simplest" data sets was difficult.²²⁹ TSA is incorporating its Alien Flight Student Program (AFSP) information into the Framework, although this only contains information from foreign nationals, and thus is less challenging to integrate than others which include the information of U.S. citizens.²³⁰ ICE is feeding its Student and Exchange Visitor Information System (SEVIS) data into the new construct, and is exploring how to connect the Investigative Case Management module of the TECS system into the broader Data Framework.²³¹

Although I&A, USCG-Intel, CBP, TSA, and ICE appear to be working to ensure that the Data Framework is a success, several other Components are not embracing it as actively. NPPD did not have any plans to use any modules of the DHS Data Framework (Neptune, CEI, or Cerberus), according to its responses to the Committee.²³² Furthermore, in order to ensure interoperability with IC ITE, NPPD told the Committee it would "rely on DHS IT support and coordination with I&A counterparts."²³³ USCIS told the Committee only that it planned to use the Data Framework interfaces for "identity resolution to gain further information on other holdings."²³⁴ This vague response seems to corroborate a senior DHS official's view that, as of late spring 2016, USCIS was not taking timely action to ensure the tagging of their data in accordance with DHS Data Framework standards.²³⁵ This same official later clarified in early September 2016 that USCIS had since taken the necessary steps, appropriately treating the Data Framework as a Departmental priority.²³⁶ FEMA responded that the Data Framework systems were "not applicable" to its CIP.²³⁷ The USSS and OCSO did not respond to the Committee's inquiries regarding its use of the new system.²³⁸ OPS told the Committee that it did not use or anticipate using any of the Data Framework systems, although it was involved in initial discussions regarding the incorporation of Component data sets.²³⁹ When pushed by Committee staff members, OPS personnel suggested that they would serve as "customers only" of the Data Framework, not incorporating their situational awareness reports into the system.²⁴⁰ Integrating all available DHS information systems into the Data Framework would greatly alleviate the previously discussed IT challenges the Department faces, and remains a pressing task.

Recommendation: The CINT should continue to aggressively incorporate new data into the DHS Data Framework, and ensure that all CIPs both contribute their data sets and employ the system to the utmost of their abilities.

VII. Intelligence Enterprise Sharing with State, Local, Tribal, and Territorial Authorities

Ensuring a consistent and reliable flow of intelligence between the federal government and SLTT authorities is a critical homeland security priority. One study found that almost 80% of foiled terrorist plots directed against U.S. interests from 1995 to 2012 were foiled due to the observations of law enforcement authorities or the general public.²⁴¹ Conversely, the same report found that “state and local resources are still commonly underutilized” for CT purposes, as of early 2016.²⁴² Despite significant improvements since 9/11 with regard to DHS’ interface with non-federal authorities, there remain major gaps in the Department’s ability to interact with SLTT organizations.

80% of foiled terrorist plots directed against U.S. interests from 1995 to 2012 were foiled due to the observations of law enforcement authorities or the general public.

**THE HANDBOOK OF THE CRIMINOLOGY
OF TERRORISM**
2016

There is a general perception from SLTT authorities that they rarely receive specific, “actionable” threat information from the IC – with DHS being their most important conduit for such warnings – according to a RAND report consolidating the 2013 discussions of a variety of intelligence professionals.²⁴³ An early 2012 survey of 71 fusion centers revealed that almost half described other law enforcement organizations as the best source of CT intelligence, followed by JTTFs, and then the reporting of local citizens and groups.²⁴⁴ That the Department did not score among the top potential sources of intelligence may have to do with a perception that even appropriately cleared SLTT authorities often have difficulty getting relevant DHS information, occasionally due to a lack of physical access or geographical distance between them and the nearest information terminal.²⁴⁵ The above results mirror a 2011 survey of the Major Cities Chiefs Association Intelligence Unit Commanders group, who also identified information provided by normal citizens, other law enforcement officers, and FBI-led JTTFs as the most important sources of counterterrorism information.²⁴⁶ Although these data are several years old, their consistency suggests the Department’s might be struggling to meet some SLTT law enforcement organizations need for intelligence.

Recommendation: The CINT should develop a consistent methodology for measuring the DHS IE’s effectiveness with regard to sharing intelligence with all SLTT authorities nationwide.

POLICY ISSUES

The CINT has a variety of responsibilities with regard to SLTT information sharing. The Homeland Security Act required DHS to “disseminate, as appropriate, information analyzed by the Department to agencies of State and local governments...in order to assist in the deterrence, prevention, preemption of, or response to, terrorist attacks against the United States.”²⁴⁷ Statute also requires that the CINT maintain a “State, Local and Regional Fusion Center Initiative to establish partnerships with local, State and regional fusion centers.”²⁴⁸ Under this official’s auspices, DHS is further responsible for coordinating “training and other support to...State and local governments that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.”²⁴⁹ The Deputy Under Secretary for Intelligence and Analysis/State and Local Program Office provides “strategic oversight of field intelligence activities,” and “serves as the “primary conduit for engagement between the DHS IE” and domestic DNI Representatives as well as SLTT and private sector partners.”²⁵⁰

More than 15 years after 9/11, however, significant confusion remains with regard to the proper intelligence flows between the federal government and SLTT authorities. Some DHS employees expressed frustration to the Committee that DHS Components did not fully inform them regarding what types of information they were sharing with SLTT law enforcement authorities.²⁵¹ One former DHS official went as far as to tell the Committee that previous I&A efforts to provide intelligence support SLTT authorities had “gone by the wayside,” in the view of some State and local law enforcement organizations. He described their “level of angst” with regard to this trend as “increasing, not subsiding.”²⁵²

Personal Relationships

As noted previously, OPS employees described their relationship with SLTT law enforcement personnel as representing “a coalition of the willing.”²⁵³ This language is identical to that used by (presumably different) OPS employees in a 2009 DHS Office of Inspector General (OIG) investigation examining a similar issue.²⁵⁴ That personnel from the same component used the same language to describe information-sharing relationships – seven years apart – indicates that certain cultural attitudes with regard to personal relationships remain unchanged in the Department. One senior DHS official responsible for field intelligence operations told the Committee that the Department’s ability to access SLTT law enforcement data “all comes down to relationships.”²⁵⁵ A 2013 GAO report regarding local intelligence sharing highlighted that successful coordination “depends most on personal relationships and can be disrupted when new leadership takes over at an entity.”²⁵⁶ This finding echoes both previous investigative work that the Committee has conducted, as well as more recent discussions with several former DHS officials.²⁵⁷ Previous Committee oversight work identified a “large body of anecdotal evidence” which indicates “to some extent even the DHS Components’” relationship with individual fusion centers – detailed below – remains largely based on personal relationships established in the field.²⁵⁸

As noted earlier in this report, personal relationships can certainly help enable the flow of terrorism-related intelligence, when built over a commonly-accepted institutional framework. A heavy reliance on trust between individuals rather than institutions, however, can slow the flow of critical information in some cases. ICE HSI-Intel officials, for instance, expressed to the Committee their hesitation in sharing some information to a wide SLTT distribution list due to a concern for leaks of sensitive material.²⁵⁹ Normalizing procedures for dissemination of intelligence to and from SLTT authorities is thus an important task for the DHS IE.

Fusion Centers

In 2013, the Committee examined the role of State and major urban area fusion centers in depth.²⁶⁰ Fusion centers, owned and operated by State and local governments, have been a cornerstone of terrorism-related intelligence sharing efforts between the federal government and SLTT authorities. In 2007, Congress authorized DHS to provide grants to fusion centers that pursue a “broad counterterrorism approach” to their operations.²⁶¹ Beginning in 2006, I&A began detailing intelligence officers to fusion centers, eventually following them with Reports Officers specifically dedicated to channeling SLTT-derived information back to I&A. The Department had employees deployed to 64 of the 78 national fusion centers as of August 2016.²⁶² Approximately 30 fusion centers have MOUs for intelligence sharing with DHS, but unfortunately there is no standardized format for such agreements, because of variation between state laws.²⁶³ A 2014 DHS report suggests that a wide consensus of agencies believe fusion center integration with the federal government has improved over time, although this is through the lens of the Department itself.²⁶⁴ DHS still, however, does not systematically capitalize on fusion centers as potential sources of information or serve them consistently as a provider of national-level terrorism-related intelligence. Although an in-depth evaluation of fusion centers themselves with regard to CT efforts is outside the scope of this report, determining how they exchange intelligence with the Department was an important goal of the Committee’s review.²⁶⁵ We will continue oversight efforts with regard to this critical topic.

The Department has taken steps to resolve some of the previous challenges that hampered intelligence sharing with fusion centers. One issue identified in the Committee’s 2013 report was that I&A Intelligence Officers and Reports Officers assigned to fusion centers across the country communicated with different offices at DHS headquarters, creating “two different chains of command.”²⁶⁶ An April 2015 restructuring of the State and Local Programs Office (SLPO) created the I&A Field Operations Division, fixing this problem by consolidating both Intelligence Officers and Reports Officers under the auspices of one organization.²⁶⁷ Furthermore, this reorganization assigned deployed I&A personnel to a geographic region, which are aligned with those that the ODNI uses.²⁶⁸ This allows I&A to collect and disseminate unique SLTT and private sector information more efficiently while avoiding the issues inherent to a fragmented management structure.

U/SIA Taylor and his staff have demonstrated a reinvigorated interest in the valuable intelligence to which fusion centers often have access. Nevertheless, the Committee has detected a trend with regard to the Department’s treatment of reporting from fusion

centers, one that emphasizes sheer numbers of production, rather than relevance or usefulness.²⁶⁹ One outside observer corroborated this to the Committee, explaining that some fusion centers have “checked the box” by providing weather reports and other very basic information in order to meet production quotas imposed by I&A in order to meet certain grant requirements.²⁷⁰ A former senior DHS official observed to the Committee that this behavior is two-way, explaining that I&A has established a trend of only establishing a data flow with fusion centers where it is beneficial for I&A to do so.²⁷¹ GAO also raised concerns in a 2015 report regarding DHS evaluations of fusion centers, which DHS officials told GAO they did not plan to change.²⁷²

DHS IE members aside from I&A have demonstrated varying levels of engagement with fusion centers. As I&A is the only CIP to receive appropriated funds specifically for deploying analysts to fusion centers, it has spearheaded cooperation with them, in the view of one former DHS official. Other CIPs must pay for employees deployed to fusion centers “out-of-pocket,” and thus have lesser incentive to do so, in his view.²⁷³ A 2014 GAO report found that CBP and ICE have not developed guidance as to how they deploy analysts to fusion centers, and the Committee was unable to identify a current coherent policy for how they do so.²⁷⁴ TSA OIA, conversely, told the Committee that it always required its field-deployed employees to maintain relationships with the I&A Intelligence Officer at local fusion centers, estimating it had relationships with approximately 75% of them nationally.²⁷⁵

Recommendation: The CINT should develop a strategic plan for engagement with fusion centers that includes all CIPs and focuses on producing timely, actionable intelligence, rather than sheer numbers of reports. This plan should include a revised method for evaluating fusion centers on the same criterion.

Other State, Local, Tribal, and Territorial Information Sharing Organizations

The White House’s October 2007 *National Strategy for Information Sharing* specified that “State and major urban area fusion centers will be the focus, but not exclusive points, within the State and local environment for the receipt and sharing of terrorism information, homeland security information, and law enforcement information related to terrorism.”²⁷⁶ The lack of a single collection point for terrorism intelligence, however, has created challenges for CT efforts within the homeland. In a 2013 report, GAO found that DHS, DOJ, and other federal organizations “do not hold field-based entities accountable for coordinating with each other, nor do they assess opportunities for additional coordination.”²⁷⁷ Furthermore, local authorities in some developed urban areas – such as New York City – have highly advanced CT and intelligence capabilities at the local level. These police and first responder forces occasionally have capabilities that outstrip those of local fusion centers and operate independently of them, according to an outside observer.²⁷⁸ Rationalizing and standardizing the Department’s interface with these actors is thus an important task for the DHS IE.

The FBI’s JTTFs, which are “[m]ulti-jurisdictional task forces managed by the FBI, and include other federal and SLTT law enforcement partners which together act as an integrated force to combat terrorism,” have similar missions to many fusion centers.²⁷⁹ Some critics have

alleged that, with regard to CT efforts, “there is no indication that fusion centers – which, under DHS guidance, postdate JTTFs – were designed to operate in a complementary fashion.”²⁸⁰ A lack of information sharing and coordination between the DHS and FBI at the JTTF level has been a major source of friction, according to a 2015 review of the FBI’s post-9/11 domestic CT efforts.²⁸¹ As the FBI has broad authorities to “coordinate the clandestine collection of foreign intelligence...and counterintelligence activities inside the United States,” its JTTFs have a unique ability to collect terrorism-related intelligence domestically that the Department does not.²⁸² Adding to the mix, several DHS IE members, but especially ICE and CBP, serve key roles in JTTFs, and provide them with information directly.²⁸³ Previous Committee oversight work has revealed that sharing between JTTFs and SLTT law enforcement organizations has room for improvement, as the FBI is often reticent to share information with them.²⁸⁴ Conversely, FBI officials are sometimes concerned that fusion centers or SLTT authorities may be conducting independent CT investigative work that could potentially disrupt ongoing federal investigations or miss key indicators.²⁸⁵ Normalizing the relationship between fusion centers and JTTFs is thus a critical task for improving terrorism-related intelligence sharing.

In addition to DHS employees at fusion centers and the FBI’s JTTFs, SLTT authorities can potentially interface with a variety of other federal or federally-funded entities. The Drug Enforcement Administration’s (DEA) Organized Crime Drug Enforcement Task Forces (OCDETF); the Office of National Drug Control Policy (ONDCP)’s High Intensity Drug Trafficking Area (HIDTA) Investigative Support Centers (ISC); and the DOJ’s Field Intelligence Groups (FIG) and Regional Information Sharing System (RISS) Centers all provide intelligence support to SLTT authorities, in addition to fusion centers.²⁸⁶ A 2013 GAO report found significant overlap in the activities of these entities. Specifically in the area of CT tactical analysis, the “broad missions of fusion centers as state and local entities increase the potential for redundancy in analytical activities and services” with the aforementioned federal ones.²⁸⁷ Furthermore, ICE HSI has 26 field offices throughout the United States.²⁸⁸ CBP has five operational Field Intelligence Groups (completely distinct from FBI Field Intelligence Groups), with three more forming as of late September 2016.²⁸⁹ In 2012 the FBI created a pilot program for yet another entity, known as the Joint Regional Intelligence Group (JRIG), although as of 2015, it was defunct.²⁹⁰

Coordinating the efforts of the aforementioned federal entities with those of fusion centers would go a long way towards improving information sharing. This would create “integrated fusion centers,” in one group’s analysis.²⁹¹ A 2014 GAO report similarly found that fusion centers generally viewed engagement with the FBI as helpful, and co-location with JTTFs can greatly assist in intelligence sharing efforts.²⁹² In addition to working together in the same physical location, GAO found in a separate report that when local information sharing entities have representation on each other’s governance boards, improved information sharing could result.²⁹³

Recommendation: The CINT should develop a comprehensive strategy for intelligence sharing and engagement with the following entities: JTTFs, FIGs, RISS Centers, and OCDETFs under the control of DOJ; Field Intelligence Groups administered by CBP; Field Offices of ICE; and HIDTA ISCs operating under the auspices of ONDCP.

TECHNOLOGY ISSUES

With the understandable desire to share terrorism-related intelligence as broadly as possible, a variety of actors have developed a slew of systems for doing so following the 9/11 attacks. These efforts have improved the flow of terrorism intelligence between the DHS IE and SLTT law enforcement authorities. The Department – and the broader federal government – for example, has also made significant strides with regard to its Suspicious Activity Reporting (SAR) program, and the Committee commends these steps. Challenges remain, however, especially with regard to the existence of several different and incompatible networks. The Committee has previously advocated establishing a national “Sensitive But Unclassified” system for intelligence sharing among Federal and SLTT partners, and stands by this recommendation.²⁹⁴

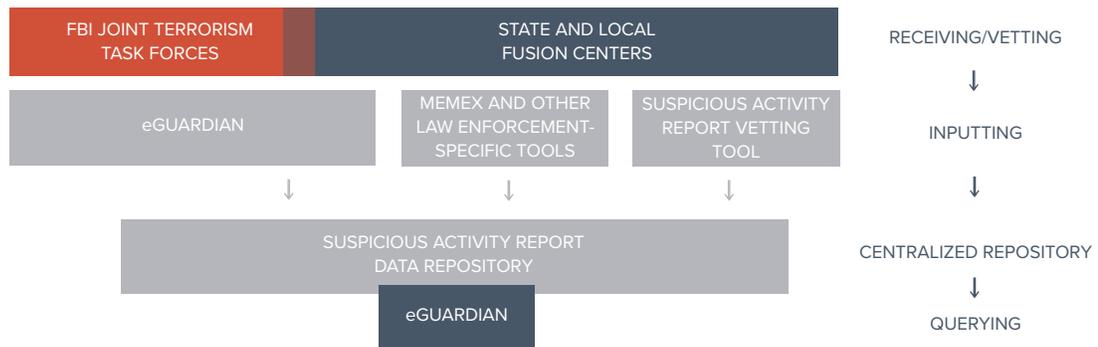
Suspicious Activity Reporting

A 2016 RAND study found that in approximately 5% of terrorist plots directed against U.S. interests from 1995 to 2012, initial clues were dropped prematurely. Either the discovering law enforcement or intelligence organization did not forward it to all relevant partners, or authorities did not conduct follow-up investigative activities.²⁹⁵ Ensuring a single repository for all leads, and that the appropriate law enforcement organization thoroughly investigates them, is thus a vital homeland security requirement. The Nationwide SAR Initiative (NSI) is a collaborative effort by DHS, FBI, and SLTT law enforcement partners to fill this need. This initiative helps law enforcement organizations to prevent terrorism by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information.²⁹⁶ The program has faced some historical challenges, although in its current form, appears to be functioning as intended.

A 2013 GAO report identified that two systems existed for the sharing of SARs; the FBI’s eGuardian and the ODNI Information Sharing Environment (ISE) Shared Space network.²⁹⁷ This report raised concerns that the FBI was not receiving all available terrorism-related information as a direct result of this dual-track system.²⁹⁸ GAO found that fusion centers, when they preferred Shared Spaces for SAR reporting, did so because of their ability to control the information in that system, as compared to the FBI’s eGuardian network. This concern was predicated on varying privacy and civil liberties restrictions between states.²⁹⁹ Unfortunately, GAO found that DOJ efforts to ensure “electronic exchanges of ISE-SARs between system” did not include “best practices for systems engineering.” Despite some “ad-hoc” testing, the systems at the time were “vulnerable to exchanging incomplete or inaccurate data.”³⁰⁰ This flaw resulted from a programming error whereby an update to one of the systems would cause a “break” in the connection, and thus prevent syncing of the two data sets.³⁰¹ A Committee study from later in 2013, however, found that the FBI had fully resolved the issue of ensuring SAR transfer between the two systems.³⁰²

On October 1, 2013, Shared Space transitioned to the SAR Data Repository (SDR). Under this new system, submitters can send terrorism SARs directly to the SDR for access via the FBI’s eGuardian system. Therefore, the new system has effectively replaced the Shared Space and removed the need for duplicate reporting within two separate systems.³⁰³ Fusion

centers use either the legacy SAR Vetting Tool (from the ISE Shared Space system), Memex or other data entry tool, or most commonly, eGuardian.³⁰⁴ JTTFs use eGuardian exclusively for submitting SARs.³⁰⁵ The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, incorporating Federal, State, and local retention policies and laws.³⁰⁶ To query the NSI SDR, all program participants use eGuardian. The FBI also took the lead for all NSI technology initiatives in January 31, 2014, to ensure that it receives all terrorism-related SARs.³⁰⁷ This new system sees significant use by all of the relevant stakeholders. For example, from October 2015 through September 2016, more than 100 SARs submitted by fusion centers have contributed to existing FBI investigations or resulted in the initiation of a new investigation, according to testimony from the Director of the National Fusion Center Association.³⁰⁸



Classified Networks

One fusion center director, who had employees with access to the full, classified Guardian system on the FBI Net enclave, went as far as to say that “until everyone is on Guardian, we aren’t there yet.” As all of his employees were deputized JTTF members, they had access to FBI terrorism information in the Guardian system.³⁰⁹ His case seems to be the exception, however, rather than the rule. Slightly over a quarter of fusion centers had FBI Net connectivity – a prerequisite for Guardian access – according to a 2012 think tank report.³¹⁰ The Department does not itself publicly report fusion center access to Guardian or identify the number with access to FBI Net.³¹¹

“Until everyone is on Guardian, we aren’t there yet.”

FUSION CENTER DIRECTOR
April 2016

The Committee notes that co-location of fusion centers with JTTFs – as was the case in the aforementioned center – more easily facilitates such access. Being in the same location allows for more effective analysis of leads submitted via the UNCLASSIFIED eGuardian platform, facilitating the vetting of SARs against classified FBI information. The aforementioned fusion center director’s comment also comports with a joint DHS, DOJ, IC, and CIA Inspector General report following the 2013 Boston Bombing, which approved of FBI efforts to encourage SLTT partners in JTTFs to review the Guardian system and share relevant threat information with their respective agencies.³¹²

Recommendation: The CINT should direct I&A to identify explicitly which fusion centers have FBI Net and Guardian Access, and engage with the FBI to ensure more widespread fusion center analyst access to the Guardian system.

In addition to FBI Net, many fusion centers have access to the DHS' SECRET Homeland Secure Data Network (HSDN).³¹³ A 2014 test of fusion center communications capabilities revealed that more than 95% had at least HSDN e-mail functionality, according to a 2014 DHS report.³¹⁴ Creating a two-way classified information flow will likely benefit both the FBI and DHS IE, as fusion centers have more consistent access to local criminal history, licensing, and motor vehicle databases.³¹⁵ Equipping fusion centers to transmit these data securely – especially between FBI and DHS classified systems – will enable more effective terrorism intelligence sharing.

Recommendation: The CINT should ensure cross-compatibility between, or at least maximum possible fusion center access to, both FBI Net and HSDN.

The Homeland Security Information Network and other UNCLASSIFIED systems

The Department operates the Homeland Security Information Network (HSIN), which it describes as the “nation’s focal point for sharing Sensitive but Unclassified information,” enabling Federal, “SLTT, International, and Private Sector homeland security partners to achieve their missions through information sharing.”³¹⁶ Initiated in 2002 under the name Joint Regional Information Exchange System (JRIES), the system became HSIN in 2004.³¹⁷ It facilitates secure instant messaging, e-mail, geospatial mapping, and workflow management in a secure (but UNCLASSIFIED) environment, which is especially useful for smaller SLTT law enforcement authorities that might not otherwise have access to such a system.³¹⁸ Previous Committee research found that HSIN had a troubled start, but has improved significantly, especially with the current version 3.0.³¹⁹ Although some outside observers have described the system as “much-maligned,” it appears to not warrant such criticism in its current form.³²⁰ One fusion centered director interviewed by the Committee was positive about HSIN, although acknowledged that it previously had significant usability issues. This director viewed the Communities of Interest (COI) and tagging capabilities of the system, combined with real-time secure chat, allowed his center to significantly improve its situational awareness regarding incidents in adjacent jurisdictions.³²¹ HSIN had more than 64,000 federal, SLTT, private sector, and international users as of August 2016, including all 78 fusion centers nationwide, and continues to grow rapidly.³²²

Many DHS CIPs have embraced HSIN as an effective method for sharing with SLTT partners. Use of the system for disseminating information, however, varies wildly throughout the Department. I&A told the Committee that it posts products to “many” of the 709 HSIN COI. I&A also uses the system to communicate with SLTT and private sector partners regarding special events, and is exploring using it for the purposes of collaborative analysis.³²³ USCG-Intel also uses HSIN, primarily for tracking transnational crime.³²⁴ DHS officials told the Committee they were exploring options to merge or consolidate HSIN with the USCG’s HOMEPORTR system.³²⁵ NPPD CIPs use the platform for sharing with SLTT authorities as well.³²⁶ TSA was highly enthusiastic about HSIN, and TSA OIA described its “TSA Intel” COI

one of the top three content providers on the HSIN-Critical Infrastructure (HSIN-CI) module in 2015.³²⁷ FEMA described HSIN as “a valuable information source,” particularly for law enforcement information. Via its Technical Assistance Program, FEMA provides fusion centers with “building capabilities and gap mitigation” on HSIN.³²⁸ OPS told the Committee that through HSIN, all of its partners are able to access the DHS COP, which provides information on ongoing and past incidents and events. The COP is highly searchable by keyword and thus easily “discoverable.”³²⁹

Other CIPs, however, are less aggressive in posting to HSIN. CBP told the Committee that it does not post products to HSIN, relying on I&A to pass them directly to SLTT authorities, leveraging relationships developed at the local level with fusion centers and law enforcement organizations.³³⁰ ICE HSI-Intelligence described its posting of products to HSIN as “limited,” and said that it only disseminated “[f]inished intelligence of general interest,” citing operational sensitivities related to ongoing investigations.³³¹ Until April 2016, USCIS FDNS did not post any products on HSIN at all, but had created its own COI as of September.³³² The USSS uses HSIN to plan and manage National Special Security Events, although did not respond to the Committee’s further inquiries regarding its use of HSIN.³³³ The OCSO did not respond specifically regarding its use of the system.³³⁴

Recommendation: CINT should determine exactly how IE members use HSIN, specifically with regard to sharing with SLTT authorities.

Recommendation: CINT should develop an IE-wide policy for what products its members should post to HSIN, and how they use the platform to collaborate with SLTT authorities.

Although DHS and other federal entities have standardized suspicious reporting procedures and now have a unified UNCLASSIFIED system architecture, there remain a variety of additional databases that SLTT authorities must use to receive and transmit information of potential CT value. The FBI’s National Crime Information Center (NCIC) is an electronic clearinghouse of criminal data accessible to most SLTT law enforcement organizations. It contains the Known or Appropriately Suspected Terrorist (KST) File, which is a critical data set for terrorism analysis.³³⁵ ICE’s Law Enforcement Information Sharing Initiative (LEISI) similarly allows law enforcement agencies to rapidly share and access data related to criminal and national security investigations. It has “connectivity” with the DOJ and is discoverable by SLTT authorities.³³⁶ The FBI’s Law Enforcement Online Enterprise Portal (LEO-EP) provides free, secure, web-based communications to SLTT authorities.³³⁷ LEO-EP and HSIN, as well as the system used by RISS centers, which are interoperable, had a total of 400,000 users between them, according to a 2015 ISE report.³³⁸ It is not clear to the Committee, however, that DHS and DOJ UNCLASSIFIED SLTT intelligence sharing networks – especially the HSIN and NCIC platforms – automatically exchange data. This interchange, or lack thereof, warrants further review.

Recommendation: The Department should conduct a review to ensure that all IE systems, and to the extent possible, those of SLTT partners, are interoperable with all relevant federally-funded databases containing terrorism information, especially those of DOJ.

VIII. Conclusion

The Department's Intelligence Enterprise "must be able to adapt to an ever evolving threat environment," dealing with challenges "that in many ways may not fit into traditional paradigms."

**JOHN COHEN, FORMER ACTING UNDER
SECRETARY FOR INTELLIGENCE AND ANALYSIS**

August 23, 2016

15 years after the 9/11 attacks, the Department has made major strides with regard to integrating the intelligence efforts of what were previously 22 different federal departments and agencies. U/SIA Taylor especially has gone the farthest of anyone holding his position in unifying and coordinating the efforts of the DHS IE. Significant difficulties remain, however, in a variety of areas. First, more clearly defining exactly what the IE comprises is an important step. Examining and more carefully focusing the missions of the various Component Intelligence Programs is second priority. Third, the CINT must work closely with the various DHS Components to share terrorism-related intelligence more effectively, both within the Department and with other federal government organizations. Finally, and most importantly for DHS IE, it must ensure that it can serve SLTT authorities effectively, while at the same time benefitting from the unique information they can provide to the Department.

Appendix I: Intelligence Enterprise Sysytems and Products

The Committee compiled the below lists of systems and products that the DHS IE uses in the conduct of its intelligence mission. The Committee examined UNCLASSIFIED parts of classified reporting (such as titles of product lines), documentation provided by the various CIPs, and open source information in compiling this list. This list is inherently incomplete, as DHS IE members varied in the level of specificity of their responses to the Committee’s questionnaire, and the name of some systems and products are themselves are classified. The below charts include hyperlinks to the appropriate reference documentation, where available.

INTELLIGENCE ENTERPRISE SYSTEMS

 UNCLASSIFIED	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Advance Passenger Information System												
Alien Flight Student Program												
All Partners Access Network												
Analytical Framework for Intelligence												
Arrival and Departure Information System												
Automated Biometric Identification System												
Automated Commercial Environment												
Automated Identification System												
Automated Indicator Sharing												
Automated Targeting System												
BorderStat												
Common Entity Index												
Central Index System												
Common Operational Picture												
Computer-Linked Application Information Management System (CLAIMS) 3												

 UNCLASSIFIED	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Computer-Linked Application Information Management System (CLAIMS) 4												
DHS Pattern Information Collaboration Sharing System												
eGuardian												
Electronic System for Travel Authorization												
Enforce Alien Removal Module												
Enforcement Case Tracking System												
Financial Crimes Enforcement Network												
HOMEPORT												
Homeland Security Information Network												
Image Storage and Retrieval System												
Intel Source												
Intelink-U												
Intelligence Records System												
Intelligence Reporting System												
Intellipedia-U												
IntelView												
Investigative Case Management System												
Investigative Information Management System												
Infrastructure Protection Gateway												
Law Enforcement Enterprise Portal												
Neptune												
OpenSource.gov												
Person Centric Query System												

<div style="display: flex; align-items: center;"> <div style="width: 15px; height: 15px; background-color: green; margin-right: 5px;"></div> UNCLASSIFIED </div>	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Refugees, Asylum, and Parole System												
Regional Information Sharing Systems (RISS) Net												
Secure Flight												
Ship Arrival Notification System												
Student and Exchange Visitor Information System												
Targeting Framework												
TECS												
Web Record Management System												
UNCLASSIFIED e-mail												
Other UNCLASSIFIED Portal												
Unspecified UNCLASSIFIED Database												
Collection Requirements Analysis Tool												
HUMINT Online Tasking and Reporting												
Intelink-S												
Intellipedia-S												
Multimedia Message System												
Tripwire Analytic Capability												
Homeland Secure Data Network (HSDN) e-mail												
TRACE e-mail												
Other SECRET Portal												
Unspecified SECRET database												

 TOP SECRET	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
<u>A-Space</u>												
<u>Cerberus</u>												
<u>CIA World Intelligence Review</u>												
Community On-Line Intelligence System for End-Users and Managers												
DSIN-TS GOLD												
Homeland Intelligence Product Repository												
Intelink-TOP SECRET												
<u>Intellipedia-TOP SECRET</u>												
<u>Library of National Intelligence</u>												
<u>National Counterterrorism Center Online</u>												
<u>Terrorist Identities Datamart Environment (TIDE) Online</u>												
TINMAN												
WebTAS												
TOP SECRET e-mail												
Unspecified TOP SECRET Portal												
Unspecified TOP SECRET database												

RAW INTELLIGENCE OR INFORMATION REPORTS

	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Daily Field Intelligence Report (DFIR)												
Field Intelligence Report												
FPS Intelligence Report												
Intelligence Information Report												
Local Information Report												
Media Monitoring Capability Report												
NOC Awareness Update Report												
Open Source Intelligence Report												
SPOT Report												
Tactical Intelligence Report												
Transportation Suspicious Incident Report												

FINISHED INTELLIGENCE PRODUCTS

	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Administrator's Daily Intelligence Briefing												
Alternative Analysis Report												
Case Analysis and Threats Summary												
Coast Guard Analytical Report												
Common Intelligence Picture												
Counterintelligence Note												
Country Threat Assessment												
Daily Cutter Support												
Daily Intelligence Briefing												

	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Daily Intelligence Summary												
DHS Senior Leader Briefing												
Encounter Analysis Report												
Field Analysis Report												
Field Intelligence Note												
FPS Exec Security Brief												
Global Regional Intelligence Digest												
Homeland Intelligence Daily												
Homeland Intelligence Today												
Homeland Security Intelligence Report												
Immigration Systems History												
Intelligence Alert												
Intelligence Assessment												
Intelligence Bulletin												
Intelligence Community Assessment												
Intelligence Note												
Intelligence Preparation of the Maritime Domain												
Intelligence Report												
Intelligence Statistical Bulletin												
Interagency Intelligence Committee on Terrorism												
Joint Intelligence Bulletin												
Lookout List												
Memorandum of Information Received												
Mission Essentials - Threat Mitigation Briefing												
Modal Threat Assessment												

	I&A	USCG	NPPD OCIA ISB	NPPD FPS TMD	CBP	TSA	ICE	USCIS	FEMA	USSS	OCSO	OPS
Monthly CINT Summary								■				
Monthly Encounter Report						■						
Monthly Newsletter								■				
National Intelligence Estimate	■											
National Terrorism Bulletin	■											
Notes to Administrator						■						
Operational Perspective and Activity												■
President's Daily Briefing	■											
Reference Aid	■											
Research Vessel List		■										
Roll Call Release	■											
Secretary Briefing Materials						■						■
Special Research Report					■							
Strategic Transportation Threat Awareness Report						■						
Tactical Intelligence Advisory		■										
Tactics, Techniques, and Procedures (TTP) Assessment						■						
Threat Assessment		■										
Transportation Intelligence Note						■						
Vessel Traffic Summary		■										

Additional Sources for Appendix I: DHS, “DHS Intelligence Enterprise Overview,” December 14, 2015; Mark A. Randol, “The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress,” Congressional Research Service, March 19, 2010; DHS OIG, “DHS’ Watchlisting Cell’s Efforts to Coordinate Departmental Nominations,” July 2013; DHS, “Arrival and Departure Information System – Information Sharing Update: DHS/CBP/PIA – 024,” March 7, 2014; I&A response to Committee questionnaire, 28 April; I&A comments on draft of Committee report, September 28, 2016; USCG-Intel response to Committee questionnaire, May 16, 2016; USCG-Intel, e-mail to Committee, June 17, 2016; NPPD response to Committee questionnaire, 28 April, 2016; CBP OI response to Committee questionnaire, 28 April 2016; DHS OIG, “Independent Review of the U.S. Customs and Border Protection’s Reporting of FY 2008 Drug Control Performance Summary Report,” February 2009; CBP, “OBIM Transition Update: Congressional Review,” April 2016; USCIS FDNS response to Committee questionnaire; TSA OIA response to Committee questionnaire, June 16, 2016; ICE comments on draft of Committee report, September 28, 2016; CBP comments on draft of Committee report, September 28, 2016; OCSO response to Committee questionnaire, May 9, 2016; OPS response to Committee questionnaire, 28 April 2016; USSS response to Committee questionnaire, May 5, 2016. Former ICE official, email to Committee, early October 2016.

Appendix II: Acronyms and Abbreviations

AFI - Analytical Framework for Intelligence
AFSP - Alien Flight Student Program
AMOC - Air and Marine Operations Center
ATO - Authority to Operate
BENS - Business Executives for National Security
BITAC - Basic Intelligence and Threat Analysis Course
BJA - Bureau of Justice Assistance
CBP - U.S. Customs and Border Protection
CEI - Common Entity Index Prototype
CGI - Coast Guard Intelligence
CHIS - Criminal History Information Sharing
CIA - Central Intelligence Agency
COI - Community of Interest
CSA - Continued Service Agreements
CT - Counterterrorism
CTAB - Counterterrorism Advisory Board
CINT - Chief Intelligence Officer
CIP - Component Intelligence Programs
COP - Common Operating Picture
DEA - Drug Enforcement Administration
DHS - Department of Homeland Security
DNI - Director of National Intelligence
DOD - Department of Defense
DOJ - Department of Justice
ECTF - Electronic Crimes Task Forces
EMS - Emergency Medical Services
ESTA - Electronic System for Travel Authorization
FBI - Federal Bureau of Investigation
FDNS - Fraud Detection and National Security Directorate
FEMA - Federal Emergency Management Agency
FIG - Field Intelligence Groups
FIR - Field Intelligence Reports
FISA - Foreign Intelligence Surveillance Act
FOUO - For Official Use Only
FPS - Federal Protective Service
FPS-TMD - Federal Protective Service Threat Management Division
FTE - Full-Time Equivalent
GAO - Government Accountability Office
GEOINT - Geospatial Intelligence
HIDTA - High Intensity Drug Trafficking Area
HOTR - Human Intelligence Online Tasking and Reporting
HSDN - Homeland Secure Data Network
HSIC - Homeland Security Intelligence Council

HSI - Homeland Security Investigations
HSIN - Homeland Security Information Network
HSRP - Homeland Security Rotation Program
HUMINT - Human Intelligence
I&A - Intelligence and Analysis
IC - Intelligence Community
ICD - Intelligence Community Directive
ICE - United States Immigration and Customs Enforcement
IG - Inspector General
IE - Intelligence Enterprise
IFM - Intelligence Functional Manager
IMM - Intelligence Mission Manager
IIR - Intelligence Information Report
IO - Intelligence Officer
IOC - Initial Operating Capability
IRAP - Intelligence Rotational Assignment Program
IRS - Intelligence Reporting System
ISB - Intelligence Support Branch
ISC - Investigative Support Centers
ISE - Information Sharing Environment
IT - Information Technology
ITE - Information Technology Enterprise
JCAT - Joint Counterterrorism Assessment Team
JDA - Joint Duty Assignment Program
JRIES - Joint Regional Information Exchange System
JTTF - Joint Terrorism Task Force
KIO - Key Intelligence Official
LEO-EP - Law Enforcement Online Enterprise Portal
LES - Law Enforcement Sensitive
MAPI - Mission Architecture and Process Innovation
MITAC - Mid-level Intelligence and Threat Analysis Course
MMC - Media Monitoring Capability
MOA - Memorandum of Agreement
MOU - Memoranda of Understanding
NCFI - National Computer Forensics Institute
NCIC - National Crime Information Center
NCTC - National Counterterrorism Center
NIP - National Intelligence Program
NJTTF - National Joint Terrorism Task Force
NOC - National Operations Center
NPPD - National Protection and Programs Directorate
NSA - National Security Agency
NSI - Nationwide Suspicious Initiative
NTAC - National Threat Assessment Center
NTC - National Targeting Center
OBIM - Office of Biometric Identity Management

OCDETF - Organized Crime Drug Enforcement Task Forces
OCIA - Office of Cyber & Infrastructure Analysis
OCSO - Office of the Chief Security Officer
ODNI - Office of the Director of National Intelligence
OFO - Office of Field Operations
OGC - Office of General Counsel
OGR - House Committee on Oversight and Government
OI - Office of Intelligence
ONDCP - Office of National Drug Control Policy
OPS - Office of Operations Coordination and Planning
OSINT - Open Source Intelligence
PII - Personal Identifiable Information
POA - Program of Analysis
PPD - Presidential Policy Directive
RBAC - Role-Based Access Control
ReCoM - Regional Coordinating Mechanisms
RFI - Request for Information
RISS - Regional Information Sharing System
RO - Report Officer
ROMC - Reports Officer Management Council
SANS - Ship Arrival Notification System
SAP - Special Access Program
SAR - Suspicious Activity Report
SBU - Sensitive but UNCLASSIFIED
SDR - Suspicious Activity Report Data Repository
SLPO - State and Local Program Office
SLTT - State, Local, Tribal, and Territorial Governments
SSI - Sensitive Security Information
TECS Mod - Treasury Enforcement Communications System Modernization
TFC - Tennessee Fusion Center
TLO - Terrorism Liaison Officer
TRACE - Transportation Security Administration Remote Access to Classified Enclave
TS/SCI - Top Secret / Sensitive Compartmented Information
TSA - Transportation Security Administration
OIA - Office of Intelligence and Analysis
TSC- Terrorist Screening Center
TTIC - Terrorist Threat Integration Center
TTP - Tactics, Techniques, and Procedures
U/S - Under Secretary
U/SIA - Under Secretary for Intelligence and Analysis
USBP - United States Border Control
USCG - United States Coast Guard
USCIS - United States Citizenship and Immigration Services
USG - United States Government
USSS - United States Secret Service
US-VISIT - United States Visitor and Immigration Status Indicator

Appendix III: Outside Groups Consulted

U.S. FEDERAL GOVERNMENT

Program Manager, Information Sharing Enterprise
Government Accountability Office
Congressional Research Service
Office of Inspector General, Department of Homeland Security
Office of the Inspector General, Department of Justice
Office of the Intelligence Community Inspector General

NONGOVERNMENTAL

Intelligence and National Security Alliance
Center for Cyber and Homeland Security, George Washington University
Business Executives for National Security
RAND Corporation

Appendix IV: Sources

- 1** National Commission on Terrorist Attacks Upon the United States, "[The 9/11 Commission Report: Executive Summary](#)," July 26, 2004, p. 21.
- 2** Brian A. Jackson, "[How Do We Know What Information Sharing Is Really Worth?](#)" (Santa Monica, CA: RAND Corporation, 2014), p.1.
- 3** Department of Homeland Security, Instruction No. 264-01-001, "DHS Intelligence Enterprise," June 28, 2013.
- 4** DHS, "[Operational and Support Components](#)," June 28, 2016. The DHS Operational and Support Components are: I&A, USCG, NPPD, CBP, TSA, ICE, USCIS, FEMA, USSS, OPS, Federal Law Enforcement Training Center, Directorate for Management, Science and Technology Directorate, Science and Technology Directorate, Domestic Nuclear Detection Office, Office of Health Affairs, and Office of Policy.
- 5** 18 United States Code (U.S.C.) § 2331 (2009).
- 6** 6 U.S.C. § 111 (2012).
- 7** 9/11 Commission, "[The 9/11 Commission Report](#)," July 22, 2004, p. 408.
- 8** Homeland Security Act of 2002, Pub. L. No. 107-296 § 201. 6 U.S.C. § 121 (2010).
- 9** Harold C. Relyea and Henry B. Hogue, "Department of Homeland Security Reorganization: The 2SR Initiative," Congressional Research Service, August 19, 2005, p. 1.
- 10** Ibid., p. 7. Foreshadowing some of the problems with which DHS still struggles, 2SR also found that "the Department has more than 10 different intelligence offices."
- 11** 6 U.S.C. §121. 9/11 Commission, "[Report](#)," p. 408.
- 12** 6 U.S.C. § 121(b) (2010).

13 DHS, Management Directive No. 264-01, “Intelligence Integration and Management,” June 12, 2013.

14 Ibid.

15 DHS Management Directive 264-01. DHS Management Directive No. 8110, “Intelligence Integration and management,” 2006.

16 DHS, “Homeland Security Intelligence Counsel Charter,” September 2015. ICE HSI-Intel briefing to the Majority Staff of the Homeland Security Committee, August 4, 2016.

17 CINT Staff comments on draft of Committee report, September 28, 2016.

18 I&A response to Committee questionnaire, April 28, 2016, p. 25.

19 I&A response to Committee questionnaire, April 28, 2016, p. 25. CINT Staff comments on draft of Committee report, September 28, 2016.

20 CBP OI briefing to Committee, August 2, 2016.

21 TSA OIA briefing to Committee, August 2, 2016.

22 Although itself not established in law, the HSIC conducts many functions that Congress has explicitly assigned to I&A. U.S.C. § 121(d)(17) to (20) and (23) (2010).

23 Charles Allen, interview with Committee, February 1, 2016.

24 GAO, “[DHS Intelligence Analysis: Additional Actions Needed to Address Analytical Priorities and Workforce Challenges](#),” June 2014, p. 8. The DHS

Intelligence Enterprise came into existence in 2006. DHS, “Intelligence Enterprise Strategic Plan,” January 2006.

25 6 U.S.C. § 121(b)(2) (2007). CINT Staff briefing to the House Committee on Homeland Security, January 15, 2016. DHS’ Under Secretary for Intelligence and Analysis in fact has four additional roles: Chief Intelligence Officer, Counterterrorism Coordinator, Counterintelligence Executive, and Departmental Information Sharing and Safeguarding Executive. CINT Staff briefing to the Committee, August 5, 2016. CINT Staff comments on draft of Committee report, September 28, 2016.

26 DHS Component briefing to Committee, early August, 2016. DHS Component legislative affairs employee, early September 2016.

27 DHS document entitled “DHS IE Overview,” December 14, 2015. The CINT Staff subsequently retracted the document, sending the Committee a new one which characterized USSS, OCSO, and OPS as HSIC members, but not IE members. I&A legislative affairs, e-mail to Committee, October 5, 2016.

28 GAO, “[DHS Intelligence Analysis](#),” p. 8.

29 CINT Staff briefing to Committee, August 5, 2016.

30 CINT Staff comments on draft of Committee report, September 28, 2016.

31 USSS legislative affairs personnel, phone conversation with Committee, April 19, 2016. OCSO comments on draft of Committee report, September 28, 2016.

32 OPS response to Committee questionnaire, 28 April 2016, p. 3.

33 DHS Privacy Office, “[2015 Data Mining Report to Congress](#),” February 2016, p. 51.

34 DHS, Instruction No. 264-01-001.

35 Implementing Recommendations of The 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 502(a)(2). DHS, Instruction No. 264-01-001. Intelligence Components are responsible for the “collection, processing, analysis, and dissemination of information within the scope of the information sharing environment, including homeland security information, terrorism information, weapons of mass destruction information, and national intelligence...in support of the intelligence mission of the Department, as led by the Under Secretary for Intelligence and Analysis.” Homeland Security Act of 2002, Pub. L. No. 107-296 § 207(1).

36 DHS OGC disputed that there was confusion with regard to the definition of CIPs, instead characterizing the lack of any authoritative count as being a matter of policy disagreement. Furthermore, OGC highlighted that from its “designated role in [DHS policy] for resolving questions of the standard’s applicability to CIPs, and the fact that no such question has been referred to OGC...it would appear there is nothing to indicate that confusion/uncertainty is the underlying problem.” The fact that such policy disagreements or lack of consensus remains more than 10 years after the formation of the IE amounts to “confusion,” in the Committee’s view. DHS OGC comments on draft of Committee report, September 28, 2016.

37 DHS Management Directive No. 264-01, 2013, p. 3. Employees of the GS-0132 Intelligence Series fill “positions concerned with advising on, administering, supervising, or performing work in the collection, analysis, evaluation,

interpretation, and dissemination of information on political, economic, social, cultural, physical, geographic, scientific, or military conditions, trends, and forces in foreign and domestic areas that directly or indirectly affect the national security.” OPM, “[Position Classification Standard Flysheet for Intelligence Series, GS-0132](#),” April 1960.

38 The intelligence cycle includes five steps: Planning and Direction, Collection, Processing, Analysis and Production, and Dissemination. CINT Staff briefing to Committee, August 5, 2016. Upon review of this report, the CINT Staff retracted this characterization, and referred the Committee back to DHS Management Directive No. 264-01. CINT Staff comments on draft of Committee report, September 28, 2016.

39 CBP OI response to Committee questionnaire, 28 April 2016, p. 2.

40 CBP OI briefing to Committee, August 2, 2016. CINT Staff briefing to Committee, August 5, 2016.

41 TSA OIA Briefing to Committee, August 2, 2016.

42 TSA OIA response to Committee questionnaire, June 16, 2016, p. 11. TSA comments on draft of Committee report, September 28, 2016.

43 I&A legislative affairs, e-mail to Committee, October 5, 2016.

44 Especially illustrative of the uncertainty with regard to the quantity and composition of CIPs is the fact that CINT Staff members briefed the Committee in August 2016 that they were in the process of determining whether USCIS had one or two CIPs, but never mentioned the possibility of a third.

CINT Staff briefing to Committee, August 5, 2016. USCIS comments on draft of Committee report, September 28, 2016. I&A legislative affairs, e-mail to Committee, October 5, 2016.

45 ICE HSI-Intel briefing to Committee, August 4, 2016. OPM, "[General Schedule Qualification Standards: Criminal Investigation Series, 1811](#)," accessed August 26, 2016.

46 CINT Staff briefing to Committee, January 15, 2016.

47 CINT Staff briefing to Committee, August 5, 2016. The CINT Staff provided a document to the Committee in early October 2016 identifying the IE as having 13 CIPs. Furthermore, they indicated that the CINT had approved all of these CIP designations, and these organizations alone made up the Intelligence Enterprise. The CINT Staff was circulating this list of designations to the Component heads for their approval as of the release of this report. I&A legislative affairs, e-mail to Committee, October 5, 2016.

48 CINT Staff briefing to Committee, August 5, 2016.

49 The Committee notes that even using this definition, what constitutes a CIP necessarily evolved over the course of the investigation. Whenever possible, we have explicitly identified when changes have occurred as well as their effective dates.

50 CINT Staff briefing to Committee, August 5, 2016. CINT Staff comments on draft of Committee report, September 28, 2016.

51 CINT Staff briefing to Committee, January 15, 2016.

52 DHS Under Secretary for Intelligence and Analysis Francis Taylor, interview with Committee, August 5, 2016.

53 Senior DHS official 1, interview with Committee, early August 2016.

54 NPPD briefing to Committee, August 3, 2016.

55 TSA OIA briefing to Committee, August 2, 2016.

56 ICE HSI-Intel briefing to Committee, August 4, 2016.

57 Ibid.

58 Senior DHS official 1, interview with Committee, early August 2016.

59 TSA OIA briefing to Committee, August 2, 2016.

60 CINT Staff briefing to Committee, January 15, 2016. DHS, Intelligence Enterprise Policy Directive 8310, February 21, 2007.

61 Senior DHS official 1, interview with Committee, early August 2016. I&A contested Component concerns regarding the speed of RFI facilitation, and provided comprehensive statistics regarding substantiating its objection. For Fiscal Year 2016, I&A reported that it delivered responses to Components an average of 0.2 days later than the requested "suspense date." CINT Staff comments on draft of Committee report, September 28, 2016. I&A legislative affairs, e-mail to Committee, October 5, 2016.

62 Outside observer 1, interview with Committee, early March 2016.

63 CBP comments on draft of Committee report, September 28, 2016.

64 President George W. Bush, Executive Order 13470, "[Further Amendments to Executive Order 12333, United States Intelligence Activities](#)," Federal Register, v. 73 no. 150, (August 4, 2008): section 4.h.16.

65 CBP OI briefing to Committee, August 2, 2016.

66 U/SIA Taylor, interview with Committee, August 5, 2016.

67 [Executive Order 13470](#), section 1.3.b.18.

68 In the interim, the Components and CINT Staff have designated some additional ones and eliminated others.

69 I&A response to Committee questionnaire, 28 April, p. 3.

70 Business Executive for National Security, "[Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties](#)," February 2015, p. 24-25. See 6 U.S.C § 121(d) (2010) for a complete list of I&A's duties.

71 A former congressional staff member with previous experience overseeing the Department attributed this incongruence between I&A's actual mission and the one codified into law to two causes. First, I&A's modern statutory authorities include some that are applicable to the DHS Office of Infrastructure Protection, currently part of NPPD, which had previously resided with I&A in the former Directorate for IAIP. At least four of the 25 aforementioned functions are exclusively related to these infrastructure protection authorities, in his view. Second, during the 2002-2004 timeframe, many of the intelligence-related

responsibilities that Congress assigned to DHS in the Homeland Security Act were instead delegated by the President to the CIA -run Terrorist Threat Integration Center ("TTIC") (which eventually became the National Counterterrorism Center) and the FBI -led Terrorist Screening Center. Christian Beckner, e-mail to Committee, September 27, 2016.

72 U.S.C. § 121(d)(1) (2010).

73 The Committee recognizes that DHS' AIC already conducts some of these functions, especially with regard to identifying and collating new data sources. The AIC would fall under the proposed Office of Strategic Intelligence. DHS, document entitled "DHS Intelligence Enterprise Overview," December 14, 2015.

74 USCG-Intel response to Committee questionnaire, May 16, 2016.

75 NPPD response to Committee questionnaire, 28 April, 2016, p. 1.

76 Cybersecurity and Infrastructure Protection Agency Act of 2016, H.R. 5390, 114th Congress (2016). DHS, "NPPD Transition Plan," August 31, 2015.

77 DHS, "Cyber and Infrastructure Protection Transition Way Ahead: Fiscal Year 2016 Report to Congress," March 17, 2016, p. 3.

78 CBP OI response to Committee questionnaire, April 28, 2016, p. 2-3.

79 Ibid, p. 2.

80 CBP OI briefing to Committee, August 2, 2016. CBP OI response to Committee questionnaire, April 28, 2016, p. 2-3.

- 81** CBP OI briefing to Committee, August 2, 2016.
- 82** CBP OI response to Committee questionnaire, April 28, 2016, p. 2-3. CBP comments on draft of Committee report, September 28, 2016.
- 83** CBP OI briefing to Committee, August 2, 2016.
- 84** James Chaparro, interview with Committee, February 29, 2016.
- 85** TSA told the Committee that “OIA’s mission is to identify security risks and to prevent attacks against the transportation system.” TSA OIA Response, June 16, 2016. TSA’s web site describes OIA’s mission as being “to prevent a terrorist attack against the nation’s transportation systems by providing security and intelligence professionals with timely information.” TSA, “[Leadership and Organization](#),” accessed August 25, 2016.
- 86** TSA OIA briefing to Committee, August 2, 2016.
- 87** TSA comments on draft of Committee report, September 28, 2016. I&A legislative affairs, e-mail to Committee, October 5, 2016.
- 88** I&A legislative affairs, e-mail to Committee, October 5, 2016.
- 89** Carrie Bachner, interview with Committee, March 8, 2016.
- 90** James Chaparro, interview with Committee, February 29, 2016.
- 91** Due to the fact that USCIS only designated its three CIPs towards the end of the Committee’s review, we were unable to evaluate their mission statements and structures in depth. CINT Staff briefing to Committee, August 5, 2016. I&A legislative affairs, e-mail to Committee, October 5, 2016.
- 92** FEMA PNP office response to Committee questionnaire, May 5, 2016, p. 1.
- 93** *Ibid.*, p. 4.
- 94** The statutory authorities under which an organization exists or conducts activities does not determine whether they constitute intelligence analysis or not. Section 121 of Title 6 establishes I&A, for example, and there is no doubt that I&A is an intelligence analysis organization. U.S.C. § 121 (2010).
- 95** DHS Office of OPS response to Committee questionnaire, 28 April 2016, p. 7.
- 96** OPS response to Committee questionnaire, 28 April 2016, p. 3.
- 97** *Ibid.*, p. 5.
- 98** DHS Office of the Chief Security Officer response to Committee questionnaire, May 9, 2016, p. 1.
- 99** CINT Staff briefing to Committee, August 5, 2016. USSS, “[Leadership](#),” accessed August 26, 2016.
- 100** CINT Staff briefing to Committee, August 5, 2016. USSS, “[Leadership](#),” accessed August 26, 2016. CINT Staff comments on draft of Committee report, September 28, 2016.
- 101** USSS response to Committee questionnaire, May 5, 2016.

- 102** USSS, "[Frequently Asked Questions](#)," accessed August 15, 2016.
- 103** The USSS-specific carveouts are found in the Implementing Recommendations of The 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 502(a)(2) and DHS Delegation No. 08503, which derives statutory authority from 6 U.S.C. §112 (b)(2) (2010).
- 104** Shawn Reese, "The U.S. Secret Service: History and Missions," Congressional Research Service, December 18, 2014, p. 19.
- 105** Treasury, Postal Service and General Government Appropriations Act, Pub. L. No. 101-508 (1991).
- 106** DHS, "[United States Secret Service Electronic Crimes Task Forces](#)," accessed August 16, 2016.
- 107** USSS, "[The Investigative Mission](#)," accessed August 15, 2016.
- 108** USCG, "[AIS Frequently Asked Questions](#)," May 13, 2016.
- 109** USCG, "[How AIS Works](#)," February 10, 2016.
- 110** CBP, "[Fact Sheet: APIS](#)," accessed August 24, 2016.
- 111** DHS Delegation No. 08503. Statutory authority from 6 U.S.C. § 121(d)(4) (2010).
- 112** Ibid. Statutory authority from 6 U.S.C., § 122 (2010).
- 113** DHS Directive 262-05, "Information Sharing and Safeguarding," September 4, 2014.
- 114** DHS Delegation No. 08503. Statutory authority from U.S.C. § 121(d)(19) (2010).
- 115** 6 U.S.C. § 124g (2013).
- 116** 6 U.S.C. § 124a (2015).
- 117** Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, March 4, 2003.
- 118** Ibid.
- 119** James Chaparro, interview with Committee, 29 February 2016.
- 120** John Cohen, phone call with Committee, January 11, 2016. James Chaparro, interview with Committee, February 29, 2016.
- 121** James Chaparro, interview with Committee, 29 February 2016.
- 122** Office of the DNI, "[Intelligence Community Civilian Joint Duty Program](#)," accessed September 12, 2016.
- 123** CINT Staff Briefing to Committee, August 5, 2016.
- 124** DHS, "[Career Development](#)," August 25, 2015.
- 125** DHS Directive 264-01-004, "DHS Intelligence Integration & Management: Intelligence Rotational Assignment Program," August 20, 2014.
- 126** CINT Staff Briefing to Committee, August 5, 2016.
- 127** ICE HSI-Intel briefing to Committee, August 4, 2016. CBP OI briefing to Committee, August 2, 2016. TSA OIA response to Committee questionnaire, June 16, 2016, p. 3-4. USCIS Fraud Detection

and National Security (“FDNS”) Directorate response to Committee questionnaire, April 14, 2016, p. 8.

128 Caryn Wagner, interview with Committee, February 16, 2016.

129 John Cohen, phone call with Committee, January 11, 2016.

130 Outside observer 2, interview with Committee, early June 2016. Outside observer 2 has had significant experience in the Intelligence Community as well as DHS.

131 Ibid.

132 ICE HSI-Intel briefing to Committee, August 4, 2016.

133 OPS briefing to Committee, August 10, 2016.

134 DHS Delegation No. 08503, “Delegation to the Under Secretary for Intelligence and Analysis/Chief Intelligence Officer,” August 10, 2012. Statutory authority from 6 U.S.C. § 122 (2010).

135 DHS Delegation No. 08503. Statutory authority from 6 U.S.C. §112 (b)(2) (2010).

136 Department of Homeland Security, Management Directive No. 0450.1, “Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA),” January 24, 2003.

137 Ms. Wagner conceded that there were likely MOUs into which CIPs had entered that she and her staff did not know about. Caryn Wagner, interview with the House Committee on Homeland Security, February 16, 2016.

138 Christian Beckner, interview with Committee, January 29, 2016.

139 CINT Staff briefing to Committee, January 15, 2016. DHS further elaborated regarding its MOU tracking efforts, writing to the Committee: “In 2015, DHS formalized the Data Access Review Council (DARC) which coordinates the oversight and compliance review of ISAAs [Information Sharing Access Agreements] involving the internal or external transfer, in bulk, of personally identifiable information (PII) in support of the Department’s national and homeland security missions. The DARC ensures the CINT has the visibility and oversight of these ISAAs. DHS is also updating the ISAA Guidebook which outlines the process for creation of ISAAs for data that may involve sharing terrorism information, homeland security information, law enforcement information and other information relevant to homeland security. The updated ISAA Guidebook is expected to be completed 2nd Quarter FY 2017.” I&A legislative affairs, e-mail to Committee, November 16, 2016.

140 Ibid.

141 Component briefing to Committee, early August 2016. DHS, “Interim Guidance for Entering Into and Executing Information Sharing Agreements with Elements of the Intelligence Community,” July 9, 2015.

142 Component briefing to Committee, early August 2016.

143 Component response to Committee questionnaire, mid-June 2016.

144 Component response to Committee questionnaire, late April 2016.

145 Ibid.

146 Component briefing to Committee, early August 2016.

147 A 1995 memo by then-Deputy Attorney General Jamie S. Gorelick built a figurative “wall” between counter-intelligence and law enforcement operations. The purpose of this move was to prevent any appearance that the FBI was using the Foreign Intelligence Surveillance Act (“FISA”) to avoid legal safeguards applicable to criminal investigations. The procedures detailed in the memo, above and beyond statutory requirements, limited information sharing between the FBI agents conducting criminal investigations and those focused on counterintelligence. The FBI was thus unable to link the collective knowledge of its own agents in the field to national priorities such as counterterrorism. Consequences of this policy included the inability of the FBI to connect the 2000 bombing of the navy ship U.S.S. Cole to Khalid al-Mihdhar, one of the eventual hijackers of American Airlines Flight 77 during the September 11, 2001 terrorist attacks. U.S. Attorney General John D. Ashcroft later stated that the guidelines set in Gorelick’s 1995 memo impeded counterterrorism efforts prior to the 9/11 attacks by restricting the FBI from mixing intelligence and criminal investigations. A 2002 special federal appeals court ruled that the USA PATRIOT Act effectively destroyed this “unnecessary...wall.” Jamie Gorelick, “[Instructions on Separation of Certain Foreign Counterintelligence, and Criminal Investigations,](#)” United States Department of Justice Office of the Deputy Attorney General, April 10, 2004. Neil A. Lewis, “[Rule Created Legal ‘Wall’ To Sharing Information,](#)” The New York Times, April 13, 2004. Dan Eggen and Walter Pincus, “[Ashcroft’s Efforts on Terrorism Criticized,](#)” Washington Post, April 14, 2004.

148 Joby Warrick, “[CIA: Systemic failures led to suicide attack,](#)” The Washington Post, October 20, 2010.

149 Leon E. Panetta, “[Message from the Director: Lessons from Khowst,](#)” October 19, 2010.

150 CINT Staff briefing to Committee, 5 August 2016.

151 Brian Jenkins, interview with Committee, March 2, 2016.

152 DHS, “[Cross U.S. Borders,](#)” accessed August 30, 2016.

153 Carrie Bachner, interview with Committee, March 8, 2016.

154 I&A briefing to Committee, June 28, 2016.

155 CINT Staff briefing to Committee, August 5, 2016.

156 Ibid. I&A legislative affairs, e-mail to Committee, November 16, 2016.

157 CINT Staff briefing to Committee, January 15, 2016,

158 CINT Staff briefing to Committee, January 15, 2016. CINT Staff comments on draft of Committee report, September 28, 2016.

159 CBP OI briefing to Committee, August 2, 2016. CBP did not comment on the Human Derived Intelligence Working Group, as it did not exist at the time of this briefing.

160 CBP legislative affairs personnel e-mail to Committee, September 1, 2016.

161 Outside observer 2, interview with Committee, early June 2016.

162 CBP officers generally author FIRs to release raw, unevaluated information that other operational personnel should know about. This could include press reporting, environment observations by CBP officers, and similar atmospheric observations. FIRs are also not necessarily related to enforcement actions. CBP OI briefing to Committee, August 2, 2016.

163 CBP OI briefing to Committee, August 2, 2016.

164 USCG-Intel response to Committee questionnaire, May 16, 2016, p. 25-26.

165 CINT Staff briefing to Committee, January 15, 2016.

166 ICE HSI-Intel response to Committee questionnaire, 18 May 2016, p. 9.

167 DHS OIG, "[ICE and USCIS Could Improve Data Quality and Exchange to Help Identify Potential Human Trafficking Cases](#)," January 4, 2016, p. 3-5.

168 Ibid., p. 12. ICE told the Committee that a "Joint Working Group is addressing the policy and legal concerns prohibiting sharing this data but USCIS still has significant systems shortfalls before ICE can receive the data reliably." ICE comments on draft of Committee report, September 28, 2016.

169 DHS OIG, "[ICE and USCIS Could Improve](#)," p. 3.

170 Louise I. Shelley, "[ISIS, Boko Haram, and the Growing Role of Human Trafficking in 21st Century Terrorism](#)," The Daily Beast, December 26, 2014. Nathan Vardi, "[Al-](#)

[Qaeda's New Business Model: Cocaine And Human Trafficking](#)," Forbes, December 18, 2009.

171 CINT Staff briefing to Committee, August 5, 2016.

172 ICE HSI-Intel briefing to Committee, August 4, 2016.

173 Ibid.

174 James Chaparro, interview with Committee, February 29, 2016.

175 ICE HSI-Intel briefing to Committee, August 4, 2016.

176 Component legislative affairs office, e-mail to Committee, late June, 2016. CIA, "[Establishment of the DNI Open Source Center](#)," November 8, 2005.

177 CINT Staff briefing to Committee, August 5, 2016.

178 CBP OI briefing to Committee, August 2, 2016. CBP draws a stark distinction between IIRs and FIRs, which it considers "a law enforcement report documenting what an officer determines is important information to file based on what they glean from enforcement operations, interviews and research under their law enforcement authorities." CBP comments on draft of Committee report, September 28, 2016. The Committee understands CBP's perspective, but contends that information contained in FIRs could have intelligence value that CBP may not identify, but another organization might. Thus, ensuring discoverability of all DHS-derived data to those with a need-to-know should be every CIPs ultimate goal.

179 TSA OIA briefing to Committee, August 2, 2016.

180 OPS briefing to Committee, August 10, 2016.

181 I&A told the Committee that we were “confusing actual “open source intelligence collection” and “media monitoring”, which is what the NOC [part of OPS] does, and is not an intelligence activity.” I&A continued, asserting that it “and OPS had to go before Congress to explain the differences between the two, as I&A had been viewed to be acting outside of its lawful scope.” CINT Staff comments on draft of Committee report, September 28, 2016. The Committee reviewed testimony from a 2012 hearing in which the Director of OPS testified, and provided it to I&A legislative affairs personnel to determine if this was the hearing in question. I&A responded that it was unable “to cite the specific hearing, but did recall that it was in 2012.” I&A comments on draft of Committee report, September 28, 2016. DHS, [Statement of Richard Chávez, Director, Office of Operations Coordination and Planning](#), before the U.S. House of Representatives Committee on Homeland Security at the Hearing entitled “DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy,” 112th Congress (2012). I&A legislative affairs, e-mail to Committee, October 5, 2016.

182 6 U.S.C. § 124a (2015).

183 CINT Staff briefing to Committee, August 5, 2016.

184 CINT Staff members expressed doubt, however, that they were seeing the full scope of CIP production, as of early August 2016. Ibid.

185 John Cohen, e-mail to Committee, August 23, 2016.

186 TSA OIA briefing to Committee, August 2, 2016.

187 TSA OIA to Committee questionnaire, June 16, 2016, p. 11.

188 John Cohen, phone call with Committee, September 1, 2016.

189 NPPD-OCIA, “Inspire Magazine Sector Threat Focus,” December 2015. SITE Intelligence Group, [“AQAP Focuses on ‘Professional Assassinations’ in 15th Issue of Inspire,”](#) accessed August 26, 2016.

190 FPS-TMD, document entitled “FPS Exec Security Brief,” June 14, 2016. Committee, [“Terror Threat Snapshot,”](#) accessed August 26, 2016.

191 NPPD briefing to Committee, August 5, 2016.

192 BENS, [“Domestic Security,”](#) February 2015, p. 6.

193 U/SIA Taylor, phone call with Committee, January 8, 2016.

194 I&A response to Committee questionnaire, April, 2016, p. 25.

195 John Cohen, e-mail to Committee, August 23, 2016.

196 Brian A. Jackson, [“How Do We Know What Information Sharing Is Really Worth?”](#) (Santa Monica, CA: RAND Corporation, 2014), p. 5.

197 USCG-Intel response to Committee questionnaire, May 16, p. 17-18.

198 CBP OI response to Committee questionnaire, 28 April 2016, p. 9.

- 199** TSA OIA response to Committee questionnaire, June 16, 2016, p. 9.
- 200** OPS response to Committee questionnaire, 28 April 2016, p. 9.
- 201** Bridget Rose Nolan, “Information Sharing and Collaboration In The United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center,” (Doctoral Dissertation, University of Pennsylvania, 2013), p. 22-23.
- 202** Office of the Director of National Intelligence, “[Intelligence Community Directive No. 501 - Discovery and Dissemination or Retrieval of Information Within the Intelligence Community](#),” January 21, 2009, p. 2.
- 203** *Ibid.*, p. 4.
- 204** *Ibid.*
- 205** Patrick Hughes, interview with the House Committee on Homeland Security, January 14, 2016.
- 206** DHS, [Statement of Caryn Wagner, Under Secretary, Office of Intelligence and Analysis](#), before the U.S. House of Representatives Committee on Homeland Security at the Hearing entitled “The DHS Intelligence Enterprise: Past, Present, and Future,” 112th Congress (2011).
- 207** TSA OIA, document entitled “Differences between Information and Intelligence,” December 28, 2015.
- 208** The DHS definition of intelligence is from DHS Instruction No. 264-01-001.
- 209** DHS Delegation No. 08503. Statutory authority from 6 U.S.C. § 121(d)(14) (2010).
- 210** Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208.
- 211** Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, March 4, 2003.
- 212** DHS Directive 262-05.
- 213** DHS, [Testimony of Caryn Wagner, Under Secretary, Office of Intelligence and Analysis](#), before the U.S. House of Representatives Committee on Homeland Security at the Hearing entitled “The DHS Intelligence Enterprise: Past, Present, and Future,” 112th Congress (2011).
- 214** CINT Staff briefing to Committee, January 15, 2016.
- 215** DHS, document entitled “DHS Intelligence Enterprise Overview,” December 14, 2015. DHS CIO legislative affairs, phone call with Committee, September 9, 2016.
- 216** TSA OIA Briefing to Committee, August 2, 2016.
- 217** DHS told the Committee that it had vastly more “information systems” than “structured databases,” although it has designated the actual number of these systems “For Official Use Only.” DHS, “Reducing IT Duplication: Response to Public Law 114-43,” January 4, 2016. DHS CIO legislative affairs personnel, phone call with Committee, September 9, 2016.
- 218** DHS OIG, [“Evaluation of DHS’ Information Security Program for Fiscal Year 2015,”](#) January 5, 2016, p. 9, 14.

219 U/SIA Taylor, Letter to Michael McCaul, Chairman of the Committee, May 27, 2016.

220 DHS Delegation No. 08503, August 10, 2012. Statutory authority from 6 U.S.C. § 124b(a) (2007).

221 U/SIA Taylor, interview with Committee, August 5, 2016.

222 The DHS Data Framework does not have any component that operates at the SECRET level, although Cerberus can handle such data because it is certified to the TS/SCI level. DHS, "[Privacy Impact Assessment: DHS Data Framework](#)," November 6, 2013, p. 4.

223 I&A response to Committee questionnaire, 28 April, p. 17. DNI, "[IC IT Enterprise](#)," accessed August 26, 2016.

224 DHS Privacy Office, "[2015 Data Mining Report to Congress](#)," February 2016, p. 50-51. CBP, "[Electronic System for Travel Authorization](#)," accessed August 26, 2016. The seven fully-integrated data sets are the CBP's Electronic System for Travel Authorization, [Form I-94 Records](#), [Passenger Name Record](#) data, [Advance Passenger Information System](#), and [Border Crossing Information](#) system; USCIS's "[Section 1367](#)" Information Repository; and USCG's [Ship Arrival Notification System](#). I&A legislative affairs, e-mail to Committee, November 16, 2016.

225 DHS, document entitled "Data Framework," June 1, 2016.

226 USCG-Intel, e-mail to Committee, June 17, 2016. USCG, "[DHS-SANS - Ship Arrival Notification System](#)," accessed August 26, 2016.

227 CBP OI briefing to Committee, August 2, 2016.

228 U/SIA Taylor, interview with Committee, June 3, 2016.

229 TSA OIA briefing to Committee, August 2, 2016.

230 DHS, "[Privacy Impact Assessment: Data Framework Data Sets](#)," September 30, 2015, p. 6. DHS, "[Privacy Impact Assessment for the Alien Flight Student Program \(AFSP\)](#)," July 28, 2014.

231 TECS is not an acronym, but previously stood for "Treasury Enforcement Communications System." DHS, "[Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing](#)," December 22, 2010. ICE HSI-Intel briefing to Committee, August 4, 2016. ICE response to Committee questionnaire, May 18, 2016, p. 9. ICE, "[Student and Exchange Visitor Information System](#)," accessed August 26, 2016.

232 NPPD response to Committee questionnaire, April 28, 2016, p. 7. Despite NPPD's response, the Committee learned that its Automated Biometric Identification System was capable of non-real time transfer with the Data Framework as of November 2016. I&A legislative affairs, e-mail to Committee, November 16, 2016.

233 NPPD response to Committee questionnaire, April 28, 2016, p. 7.

234 USCIS FDNS response to Committee questionnaire, 14 April, 2016, p. 7.

235 Senior DHS official 2, interview with Committee, early June, 2016.

- 236** Senior DHS official 2, phone call with Committee, early September, 2016.
- 237** FEMA PNP response to Committee questionnaire, May 5, 2016, p. 5.
- 238** USSS response to Committee questionnaire, May 5, 2016. OCSO response to Committee questionnaire, May 9, 2016.
- 239** OPS response to Committee questionnaire, 28 April 2016, p. 11.
- 240** OPS briefing to Committee, August 10, 2016.
- 241** Gary LaFree and Joshua D. Freilich, pre-publication draft chapter from [The Handbook of the Criminology of Terrorism](#) (Wiley-Blackwell, anticipated publication, December 2016), available via "[Terrorist Plots Against the United States: What We Have Really Faced, and How We Might Best Defend Against It](#)," RAND Corporation, 2016, p. 13-14.
- 242** *Ibid.*, p. 3.
- 243** Brian Michael Jenkins, Andrew Liepman, Henry H. Wills, "[Identifying Enemies Among Us: Evolving Terrorist Threat and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing](#)," RAND Corporation, 2014, p. 9.
- 244** Frank J. Cilluffo, et al., "[Counterterrorism Intelligence: Fusion Center Perspectives](#)," Homeland Security Policy Institute, George Washington University, June 2012, p. 7, 15.
- 245** BENS, "[Domestic Security](#)," February 2015, p. 13-14.
- 246** Frank Cilluffo, Joseph Clark, and Michael Downing. "[Counterterrorism Intelligence: Law Enforcement Perspectives](#)," September 2011, Homeland Security Policy Institute, George Washington University, p. 10, 12.
- 247** Homeland Security Act of 2002, Pub. L. No. 107-296 § 201(d)(9).
- 248** DHS Delegation No. 08503. Statutory authority from 6 U.S.C. § 124h.
- 249** 6 U.S.C. § 121(d)(15) (2010).
- 250** DHS Directive 264-01.
- 251** I&A briefing to Committee, January 15, 2016.
- 252** John Cohen, phone call with Committee, September 1, 2016.
- 253** OPS briefing to Committee, August 10, 2016.
- 254** DHS OIG, "[Information Sharing at the National Operations Center](#)," November 10, 2009, p. 25.
- 255** I&A briefing to Committee, June 28, 2016.
- 256** GAO, "[Information Sharing: Agencies Could Better Coordinate to Reduce Overlap in Field-Based Activities](#)," April 2013, p. 34.
- 257** Committee, "[The National Network of Fusion Centers](#)," July 2013, p. 59.
- 258** *Ibid.*, p. 15.
- 259** ICE HSI-Intel briefing to Committee, August 4, 2016.
- 260** Committee, "[The National Network of Fusion Centers](#)," July 2013.

- 261** Implementing Recommendations of The 9/11 Commission Act of 2007, Pub. L. No. 110–53, § 511.
- 262** DHS, document entitled “I&A Field Operations Personnel Deployments,” September 8, 2016.
- 263** I&A briefing to Committee, June 28, 2016.
- 264** DHS, “[2014 National Network of Fusion Centers Final Report](#),” p. v.
- 265** The Committee previously found it difficult to “accurately, adequately, and tangibly measure the value of fusion centers...particularly to the counterterrorism mission.” Committee, [The National Network of Fusion Centers](#), p. v.
- 266** Committee, “[The National Network of Fusion Centers](#),” p. 52-53.
- 267** I&A response to Committee questionnaire, p. 1-2.
- 268** I&A briefing to Committee, June 28, 2016.
- 269** Ibid.
- 270** Outside observer 1, interview with Committee, early March 2016.
- 271** James Chaparro, interview with Committee, 29 February 2016.
- 272** GAO, “[Information Sharing: DHS is Assessing Fusion Center Capabilities and Results, but Needs to More Accurately Account for Federal Funding Provided to Centers](#),” November 2014, p. 12-13.
- 273** Ibid.
- 274** GAO, “[Information Sharing: DHS is Assessing Fusion Center Capabilities](#),” November 2014, p. i.
- 275** TSA OIA briefing to Committee, August 2, 2016.
- 276** Executive Office of the President, National Security Council, “[National Strategy for Information Sharing](#),” October 2007, p. A1-1.
- 277** GAO, “[Information Sharing: Agencies Could Better Coordinate](#),” April 2013, p. 45.
- 278** Outside observer 1, interview with Committee, early March 2016.
- 279** DHS, “[Fusion Centers and Joint Terrorism Task Forces](#),” July 29, 2016.
- 280** Jerome H. Kahan, “Living with Terrorism: Unimaginable Nightmare or Prospective Reality,” *Journal of Homeland Security and Emergency Management*, Vol. 12, Issue 2, May 2015, p. 246.
- 281** FBI, “[The FBI: Protecting the Homeland in the 21st Century](#),” March 2015, p. 81-82.
- 282** President George W. Bush, [Executive Order 13470](#), section 1.3.b.20.a.
- 283** FBI, “[Protecting the Homeland in the 21st Century](#),” p. 81-82.
- 284** FBI’s streamlining the procedure for releasing terrorism-related information to SLTT authorities via a revised MOU, which resulted from an examination of the 2013 Boston Marathon Bombing, is a step in the right direction. Inspectors General of the IC, DHS, CIA, and DOJ, “[Unclassified Summary of the April 15, 2013 Boston Marathon Bombings](#),” p. 26-29.

285 GAO, [“Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective,”](#) March 2013, p. 16-17.

286 Michael Downing and Matt A. Mayer, [“The Domestic Counterterrorism Enterprise: Time to Streamline,”](#) Heritage Foundation, 2012. Senate Select Committee on Intelligence, Letter #2014-0592 to Intelligence Community Inspector General, dated February 5, 2014. GAO determined that, although not their primary missions, RISS Centers and HIDTA ISCs are authorized to engage in CT efforts. GAO, [“Information Sharing: Agencies Could Better Coordinate,”](#) p. 10-11.

287 GAO, [“Information Sharing: Agencies Could Better Coordinate,”](#) p. 21, 24-25, 27.

288 DHS, [“ICE Field Offices,”](#) accessed October 5, 2016.

289 CBP OI briefing to Committee, August 2, 2016. CBP comments on draft of Committee report, September 28, 2016.

290 Downing and Mayer, [“The Domestic Counterterrorism Enterprise.”](#) FBI, [“Protecting the Homeland in the 21st Century,”](#) p. 92-93. FBI, [“Protecting the Homeland in the 21st Century,”](#) p. 92. The Committee has previously expressed concern regarding the possibly duplicative role of the proposed JRIG. Committee, [The National Network of Fusion Centers](#), p. 59.

291 BENS, [“Domestic Security Revisited: An Update on the Progress U.S. Intelligence and Law Enforcement Agencies have Made in Confronting a Dynamic Domestic Threat Landscape,”](#) March 2016, p. 10-11.

292 GAO, [“Information Sharing: DHS is Assessing Fusion Center Capabilities,”](#) p. 35.

293 GAO, [“Information Sharing: Agencies Could Better Coordinate,”](#) p. 35-37.

294 Committee, [“The National Network of Fusion Centers,”](#) p. ix.

295 LaFree and Freilich, draft chapter from [The Handbook of the Criminology of Terrorism](#) available via [“Terrorist Plots Against the United States,”](#) p. 12.

296 DOJ, Nationwide SAR Initiative (NSI), [“The Nationwide SAR Initiative,”](#) accessed August 26, 2016.

297 GAO, [“Information Sharing: Agencies Could Better Coordinate,”](#) p. 27. Nationwide SAR Initiative (NSI), [“Final Report: Information Sharing Environment \(ISE\) Suspicious Activity Reporting \(SAR\) Evaluation Environment,”](#) January 2010. FBI, [“eGuardian,”](#) accessed August 26, 2016.

298 GAO, [“Information Sharing: Additional Actions Could Help Ensure That Efforts to Share Terrorism-Related Suspicious Activity Reports Are Effective,”](#) March 2013, p. 15.

299 *Ibid.*, p. 18-20.

300 *Ibid.*, p. 26.

301 CINT Staff briefing to Committee, August 5, 2016.

302 Committee, [The National Network of Fusion Centers](#), p. 34.

303 DHS, "[Privacy Impact Assessment Update for the Department of Homeland Security Information Sharing Environment \(ISE\) Suspicious Activity Reporting \(SAR\) Initiative](#)," May 12, 2015, p. 2-3.

304 Business Wire, "[NIAC Fusion Center Adds Suspicious Activity Reporting via Memex](#)," October 24, 2011. CINT Staff briefing to Committee, August 5, 2016.

305 CINT Staff briefing to Committee, August 5, 2016.

306 NSI, "[Information Sharing Environment Functional Standard Suspicious Activity Reporting](#)," version 1.5.5, p. 2.

307 CINT Staff briefing to Committee, August 5, 2016. DHS, "[Privacy Impact Assessment Update](#)," May 12, 2015, p. 2-3.

308 Statement of Mike Sena, President, National Fusion Center Association before the U.S. House of Representatives Committee on Homeland Security at the Hearing entitled "[State and Local Perspectives on Federal Information Sharing](#)," 114th Congress (2016).

309 Fusion Center Director 1, interview with Committee, early April 2016.

310 Cilluffo, et al., "[Counterterrorism Intelligence: Fusion Center Perspectives](#)," p. 16.

311 DHS, "[2014 National Network of Fusion Centers Final Report](#)," p.7. The CINT staff also noted to the Committee that DHS personnel generally do not receive Guardian access unless they are a member of an FBI JTTF. CINT Staff comments on draft of Committee report, September 28, 2016.

312 Inspectors General of the IC, CIA, DOJ, and DHS, "[Unclassified Summary of the April 15, 2013 Boston Marathon Bombings](#)," p. 22.

313 DHS, "[IT Program Assessment – Homeland Secure Data Network \(HSDN\)](#)," accessed August 24, 2016, p. 2.

314 DHS, "[2014 National Network of Fusion Centers Final Report](#)," p. 7.

315 Cilluffo, et al., "[Counterterrorism Intelligence: Fusion Center Perspectives](#)," p. 16.

316 DHS, "[Fact Sheet - Homeland Security Information Network \(HSIN\)](#)," accessed August 25, 2016.

317 DHS OIG, "[Homeland Security Information Network Could Support Information Sharing More Effectively](#)," June 2006, p. 7. The Defense Intelligence Agency (DIA) originally operated and maintained JRIES but transferred program management of the system to DHS in September 2003, due to funding constraints. DHS, Statement of Frank W. Deffer, Assistant Inspector General, Information Technology, before the U.S. House of Representatives Committee on Homeland Security at the Hearing entitled "The Homeland Security Information Network," 109th Congress (2006).

318 DHS Homeland Security Information Network (HSIN) team briefing to Committee, August 5, 2016.

319 Committee, [The National Network of Fusion Centers](#), p. 42.

320 Matt A. Mayer, "[Consolidate Domestic Intelligence Entities Under the FBI](#)," American Enterprise Institute, March 7, 2016.

321 Fusion Center Director 1, interview with Committee, early April 2016.

322 DHS HSIN team briefing to Committee, August 5, 2016.

323 I&A response to Committee questionnaire, 28 April, p. 14-15.

324 USCG-Intel response to Committee questionnaire, p. 15.

325 DHS HSIN team briefing to Committee, August 5, 2016.

326 In 2015, OCIA-ISB posted 96 products on HSIN-CI. NPPD e-mail to Committee, August 4, 2016. FPS-TMD estimated that it had posted approximately 20 in the same year. NPPD briefing to Committee, August 3, 2016.

327 The "TSA Intel" HSIN Community of Interest (COI) attracted approximately 10.2% of the HSIN-CI membership on a monthly basis, as of August 2016. In 2016, it experienced 53,768 hits with a total of 1,591 products. TSA OIA e-mail to Committee, August 4, 2016.

328 FEMA PNP response to Committee questionnaire, May 5, 2016, p. 5.

329 OPS response to Committee questionnaire, 28 April 2016, p. 8.

330 CBP OI Briefing to Committee, August 2, 2016.

331 ICE HSI-Intel response to Committee questionnaire, 18 May 2016, p. 8.

332 USCIS FDNS response to Committee questionnaire, 14 April, 2016, p. 6. USCIS comments on draft of Committee report, September 28, 2016.

333 DHS, "[Homeland Security Information Network 2015 Annual Report](#)." USSS response to Committee questionnaire, May 5, 2016.

334 OCSO response to Committee questionnaire, May 9, 2016.

335 FBI, "[National Crime Information Center \(NCIC\)](#)," accessed August 23, 2016.

336 ICE, "[Law Enforcement Information Sharing Initiative](#)," accessed August 23, 2016.

337 FBI, "[Law Enforcement Online Enterprise Portal Makes Access More Convenient](#)," December 28, 2012.

338 Information Sharing Environment (ISE), "[2015 Annual Report to the Congress](#)," p. 3.