

OFFICE OF INSPECTOR GENERAL

DHS Can Strengthen Its Cyber Mission Coordination Efforts



Homeland
Security

OIG-15-140
September 4, 2015



DHS OIG HIGHLIGHTS

DHS Can Strengthen Its Cyber Mission Coordination Efforts

September 4, 2015

Why We Did This Audit

We audited the DHS components' coordination in performing their cyber missions. We sought to determine whether their cyber roles and responsibilities have been well delineated and a process is in place for department-wide information sharing and coordinated response to cyber incidents and criminal investigations. We also evaluated the components' compliance with applicable DHS information security requirements.

What We Recommend

We recommended that DHS develop both a department-wide cyber strategy and a security training program. DHS components must also address the information security deficiencies we identified.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

Department of Homeland Security (DHS) components have strengthened coordination in performing their cyber missions. For example, United States Immigration and Customs Enforcement (ICE) and United States Secret Service (USSS) have enhanced relationships with the National Protection and Programs Directorate's (NPPD) National Cybersecurity and Communications Integration Center to improve information sharing and coordination on incident response and investigation.

Despite these positive steps, the Department can take additional actions to improve its cyber mission coordination. For example, the Office of Policy has not developed a cyber strategic implementation plan due to its recent establishment and limited staff. Without a strategic plan, DHS cannot effectively align the components' cyber responsibilities and capabilities with DHS' overall mission.

Further, DHS needs to establish a cyber training program to provide its analysts and investigators with the skills needed to effectively perform their duties at ICE, NPPD, and USSS. An automated cyber information sharing tool is needed to enhance coordination among the components. Moreover, we identified deficiencies regarding ICE and USSS' implementation of DHS baseline configuration settings, vulnerability management, weakness remediation, and specialized security training that may result in loss, misuse, modification, and unauthorized access to the Department's information systems and data.

Management Response

DHS concurred with all nine recommendations and has implemented corrective actions to address the findings. We considered recommendations 1-5, 7, and 9 open and resolved. Recommendations 6 and 8 are open and unresolved.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

September 4, 2015

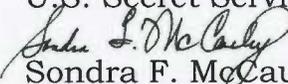
MEMORANDUM FOR: Andy Ozment
Assistant Secretary, Office of Cybersecurity and
Communications
National Protection and Programs Directorate

Rosemary Wenchel
Acting Assistant Secretary for Cyber, Infrastructure,
and Resilience
Office of Policy

Peter Edge
Executive Associate Director of Homeland Security
Investigations
U.S. Immigration and Customs Enforcement

Craig Magaw
Deputy Director
U.S. Secret Service

FROM:


Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *DHS Can Strengthen Its Cyber Mission Coordination Efforts*

Attached for your action is our final report, *DHS Can Strengthen Its Cyber Mission Coordination Efforts*. We incorporated the Department's comments in our report.

The report contains nine recommendations aimed at enhancing the program's overall effectiveness. The Department concurred with all nine recommendations. Based on information provided in your response to the draft report, we consider recommendations 6 and 8 open and unresolved. As prescribed by the Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

supporting documentation necessary to inform us about the current status of the recommendations. Until your response is received and evaluated, the recommendations will be considered open and unresolved.

Based on information provided in your response to the draft report, we consider recommendations 1-5, 7, and 9 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGTAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division, at (202) 254-5472.

Attachment



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Table of Contents

Background3

Results of Audit4

Progress in Coordinating Cyber Mission Activities5

Challenges in Cyber Mission Coordination and Response6

 DHS Must Develop a Strategic Implementation Plan
 to Improve Cyber Awareness across Components.....6

 Recommendation.....7

 DHS Has Not Established a Department-wide Cyber
 Training Program.....9

 Recommendation..... 10

 DHS Components Would Benefit from an Enterprise-wide
 Automated Capability for Sharing Cyber Information 11

 Recommendation..... 13

 Technical Enhancements Could Strengthen Cyber Mission
 Information Systems..... 14

 Recommendations 16

 ICE and USSS Are Not Compliant with Certain DHS
 Information Security Program Requirements..... 18

 Recommendations 20

Appendixes

Appendix A: Objective, Scope, and Methodology 22

Appendix B: DHS Comments to the Draft Report. 24

Appendix C: Office of Information Technology Audits Major
Contributors to This Report 30

Appendix D: Report Distribution..... 31

Abbreviations

C3	Cyber Crimes Center
CETS	Child Exploitation Tracking System
CHCO	Chief Human Capital Officer
CIDS	Criminal Investigative Division Suite
CIO	Chief Information Officer



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

CIR	Office of Cyber, Infrastructure and Resilience
CMSI	CyberSkills Management Support Initiative
DHS	Department of Homeland Security
ICE	United States Immigration and Customs Enforcement
ISSO	Information System Security Officer
NCCIC	National Cybersecurity and Communications Integration Center
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
OMB	Office of Management and Budget
PLCY	Office of Policy
POA&M	Plan of Action and Milestones
USSS	United States Secret Service



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Background

Prevalent cyber attacks, including attempts to gain unauthorized access to information systems or sensitive data stored and processed by these systems, have triggered an expansion of cybersecurity initiatives in the government and private sectors. The President has identified cybersecurity as one of the most serious economic and national security challenges we face as a Nation.

One of the Department’s missions is to coordinate national protection, prevention, mitigation of, and recovery from cyber incidents, and to oversee the protection of the Federal network (.gov). Table 1 depicts some of the core cyber responsibilities of DHS and several of its components.

Table 1. DHS’ Core Cyber Responsibilities		
ICE	NPPD	USSS
<ul style="list-style-type: none"> - Identity and benefit document fraud - Money laundering - Financial fraud - Commercial fraud - Counter-proliferation investigations - Narcotics trafficking - Illegal exports - Child exploitation - Computer forensics 	<ul style="list-style-type: none"> - Critical infrastructure protection - Intrusion detection and prevention for Federal networks - Cyber threat and vulnerability analysis dissemination - Network and digital media analysis - Coordination of national response to significant cyber incidents 	<ul style="list-style-type: none"> - Financial payment systems protection - Critical infrastructure protection - Identity theft - Credit card fraud - Bank fraud

Source: Office of Inspector General (OIG) based on documentation review and interviews with ICE, NPPD, and USSS personnel.

Specifically, DHS is responsible for coordinating the national response to cyber incidents, such as the use of phishing, malicious software, account theft, access device and bank fraud, and cyber intrusions.¹ DHS components (i.e., ICE, NPPD, and USSS) are actively involved in cybersecurity.² For example:

- NPPD is primarily responsible for fulfilling DHS’ national, non-law enforcement cybersecurity missions. It also provides crisis management, incident response, and defense against cyber attacks for Federal civil executive branch networks (.gov). National Cybersecurity and Communications Integration Center (NCCIC), which is a part of the Office of Cybersecurity and Communications, serves as a central location for

¹ Phishing is the illegal attempt to acquire sensitive information, such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

² Our review focused on Homeland Security Investigations, a sub-component of ICE, which has the authority to conduct cybercrime investigations. With respect to USSS’ cyber responsibilities, our review focused on the Criminal Investigative Division.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

operational components involved in cyber response activities to share information between the public and private sector.

- ICE focuses on criminal activities that are conducted on or facilitated by the Internet as well as cross-border cybercrimes. For example, ICE performs domestic and international investigations into cross-border smuggling of people and guns. It also investigates narcotics, financial, cyber, and immigration-related crimes.
- USSS performs investigations to identify, locate, and apprehend criminal organizations and individuals targeting the Nation's critical financial infrastructure and payment systems.

In December 2014, DHS established the Office of Cyber, Infrastructure, and Resilience (CIR) Division, within the Office of Policy, to improve information sharing and collaboration across the Department, and reduce any duplication of efforts by the components in the performance of their cyber missions.³ To achieve this goal, the Deputy Secretary tasked CIR, in coordination with the Strategy, Planning, Analysis and Risk Division, to develop cross-departmental cyber strategies to effectively capitalize on the Department's cyber capabilities and workforce.

Results of Audit

DHS components have strengthened coordination in performing their cyber missions. For example, component representatives participate in various working groups and initiatives to collaborate on cyber legislation, policies, and information sharing. Further, ICE and USSS have enhanced relationships with NPPD's NCCIC to improve information sharing and coordination on incident response and investigation.

Despite these positive steps, the Department can take additional actions to improve its cyber mission coordination. For example, CIR has not developed a cyber strategic implementation plan due to its recent establishment and limited staff. Without a strategic plan, DHS cannot effectively align the components' cyber responsibilities and capabilities with DHS' overall mission.

Further, DHS needs to establish a cyber training program to provide its analysts and investigators with the skills needed to effectively perform their duties at ICE, NPPD, and USSS. An automated cyber information sharing tool is needed to enhance coordination among the components. Moreover, deficiencies we identified in ICE and USSS' implementation of DHS baseline

³ *Strengthening Departmental Unity of Effort in Cyber Security*, issued by the Deputy Secretary on November 12, 2014.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

configuration settings, vulnerability management, weakness remediation, and specialized security training as required may result in loss, misuse, modification, and unauthorized access of the Department's information systems and data.

Progress in Coordinating Cyber Mission Activities

DHS and its components have taken steps to improve communication, collaboration, and information sharing efforts to strengthen the Department's investigation and response to cyber attacks. For example:

- USSS assigned a full-time Special Agent to the NCCIC watch floor to improve communication and information sharing with other components. Additionally, ICE has two full-time Special Agents on the NCCIC watch floor to strengthen its relationships with NPPD. Further, ICE has assigned full-time agents to both the staff of NPPD Under Secretary and Office of Policy's (PLCY) CIR. These efforts have helped improve the levels of collaboration among ICE, NPPD, and USSS regarding investigation and response to cyber incidents.
- Representatives from ICE, NPPD, PLCY, Office of Privacy, Secretary, and USSS meet weekly to collaborate on cybersecurity issues regarding information sharing legislation and automation, single portal liability and privacy protection, and data receipt, processing, and delivery.
- USSS and ICE collaboratively investigated a money laundering scheme involving an international online payment processor and money transfer system, which resulted in the theft of more than \$6 billion in funds. Agents identified 40 bank accounts located in 8 countries, which has resulted in the seizure or restraint of approximately \$40 million in assets.
- ICE, NPPD, and USSS collaborated on the investigation of a breach of the payment card system at a major retailer. Compromised information included customer names, credit and debit card numbers, card expiration dates, and card verification-value security codes. As a result of the investigation, NPPD's NCCIC shared incident details and mitigation strategies with other retailers to prevent similar attacks.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Challenges in Cyber Mission Coordination and Response

Although DHS has taken actions, the Department still faces challenges in sharing cyber information among its components. For example, due to the recent establishment of the office and limited staff personnel, CIR has not developed or implemented a cross-departmental cyber strategy and performance metrics to promote the components' awareness of and collaboration in performing their cyber missions. In addition, DHS has not established a department-wide, comprehensive training program to enhance the skillsets of cyber analysts and investigators. Instead, the components are developing their training programs independently, which could lead to inconsistent or duplicative effort and could hinder DHS from performing its cyber missions in an integrated and effective manner.

Further, we identified deficiencies in the components' compliance with DHS' information security requirements in the areas of Plan of Action and Milestones (POA&M) management, specialized training, and the implementation of DHS baseline configuration settings. If not addressed, these deficiencies could result in the loss, misuse, modification, and unauthorized access to the Department's information systems and data.

DHS Must Develop a Strategic Implementation Plan to Improve Cyber Awareness across Components

ICE, NPPD, and USSS cyber personnel do not have a clear understanding of each other's responsibilities and operational and investigative capabilities as needed to effectively coordinate and collaborate to fulfill DHS' cyber mission. For example, NPPD personnel indicated that they were not familiar with the breadth of ICE's cyber mission and responsibilities, which includes money laundering, financial fraud, child exploitation, and computer forensic investigations. Further, NPPD and USSS personnel shared a misconception that ICE was primarily responsible for child exploitation investigations, or were not familiar with ICE's cyber mission and capabilities in general.

This lack of understanding has led to conflicts regarding assignments and response to incidents. For example, according to selected ICE cyber analysts, there have been instances in which incidents were referred to the wrong components within DHS (USSS or ICE) or outside of the Department, including to the Department of Justice's Federal Bureau of Investigation. Ultimately, this confusion may have restricted DHS from using all of its cybersecurity capabilities or caused delays in its response and recovery efforts.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Due to the recent establishment of the office and limited staff personnel, CIR has not yet developed a strategic implementation plan that would define the components' cyber responsibilities and capabilities. According to CIR management officials, the office currently is establishing timelines for the strategic plan and policies. The office wants to ensure that it has appropriate time to coordinate with the components on developing this department-level guidance. In addition to a strategic implementation plan, CIR also has not developed performance measures and identified goals for ICE, NPPD, and USSS to accomplish the Department's cyber mission.

The *Blueprint for a Secure Cyber Future* requires DHS to unify and coordinate its response to cyber incidents, integrate information from Federal cybersecurity centers and other stakeholders, and conduct criminal and forensics investigations with other law enforcement entities.⁴ The Office of Management and Budget (OMB) requires agencies to develop strategic implementation plans to identify major functions and operations of an agency.⁵ A strategic plan should define the mission, long-term goals, and specific milestones and performance measures by which the Department will monitor its progress in addressing specific national problems, needs, or challenges related to its mission. In addition, the plan should include general goals and objectives, and a description of how those goals and objectives can be achieved.

Without a strategic implementation plan, CIR cannot ensure that DHS is effectively performing its cyber mission or ensure that components clearly understand one another's cyber responsibilities, capabilities, or key mission areas. In addition, developing a strategic implementation plan may allow DHS to align its components' cyber responsibilities and capabilities with the Department's overall mission. Further, department-wide cyber policies will allow the standardization of components' cyber activities and coordination efforts to reduce redundant capabilities and execute their programs more efficiently. Improved understanding of others' cyber missions, capabilities, and standardization of coordinated cyber activities would enable components to share actionable information to respond to and investigate incidents in a more efficient manner.

Recommendation

We recommend that the Principal Deputy Assistant Secretary for Cyber Policy:

⁴ *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, November 2011.

⁵ *Preparation and Submission of Strategic Plans, Annual Performance Plans, and Annual Performance Reports*, OMB Circular A-11, Part 6, July 2014.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 1. Develop a comprehensive, cross-departmental strategic implementation plan that defines components' cyber missions and responsibilities, including long-term goals, performance metrics, and milestones to measure progress in unifying the Department's incident response and coordination efforts.

DHS Comments to Recommendation 1

DHS concurred with recommendation 1. Although the report correctly indicates that the "PLCY has not developed a cyber strategic implementation plan due to its recent establishment and limited staff," it is worth noting that the *DHS FY 2014–2018 Strategic Plan* signed by Secretary Johnson on December 7, 2014, does establish Mission 4 – Safeguard and Secure Cyberspace. Moreover, according to OMB Circular A-11, *Preparation, Submission, and Execution of the Budget* guidance and consistent with the *GPRA Modernization Act of 2010*, the strategic plan prescribes goals, performance metrics, and planned targets associated with Mission 4 for the Department.

Additionally, since the start of fieldwork for this audit, the CIR and the Strategy Planning, Analysis and Risk Divisions have teamed to build the *DHS 2015 Cyber Strategy*. This strategy was vetted among components and Headquarters, and was submitted to the DHS senior leadership in July 2015 for approval and signature. The draft mandates development of a cyber strategy implementation plan within 90 days of the strategy's approval. The Implementation Plan will specify strategic objectives, corresponding tasks, and associated performance metrics.

The strategy also directs the establishment of a Cyber Strategy Implementation Group within 30 days, and the stand-up of a formal Cyber Advisory Board within 60 days. In the aggregate, the *FY 2014–2018 Strategic Plan* and the *2015 Cyber Strategy's Implementation Plan* will satisfy requirements for a cross-departmental strategic implementation plan. The Acting Assistant Secretary for CIR Policy will chair the Cyber Strategy Implementation Group and oversee both the development and execution of the Implementation Plan. The estimated completion date is February 29, 2016.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will remain open until DHS provides documentation to support that all planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

DHS Has Not Established a Department-wide Cyber Training Program

DHS has not established a Department-wide cyber training program for its analysts and investigators. According to the *Cybersecurity Workforce Management Support Directive*, the Executive Director of CyberSkills Management Support Initiative is required to create and oversee a comprehensive and vigorous training and professional development program.⁶ The focus of the program is to help DHS cybersecurity analysts and investigators maintain and enhance their cybersecurity skills to execute the Department's mission.

Currently, components are arranging the specialized training needed for their cyber analysts and investigators in a decentralized manner. In some instances, components are working independently with contractors to develop internal training courses and curriculums for their cyber staff. As part of these efforts, components are incurring significant, duplicative costs associated with developing and conducting independent internal training courses. For example, ICE has hired a contractor to develop four, two-week classes on basic cyber skills, investigations, undercover operations, and network intrusion for approximately \$690,000. In addition, NPPD is planning to spend \$1.9 million to develop a core cyber training curriculum, which will include incident response, forensics, network, and malware analysis across the NCCIC over the next 12 months. Further, USSS is planning to spend over \$400,000 to host an annual conference on network intrusion training.

Despite these training plans, ICE, NPPD, and USSS officials told us that budgetary constraints caused by recent continuing resolutions have limited their ability to provide their personnel with all the cybersecurity training they need. For example, an ICE analyst informed us that he has not attended any formal training in four years, in part because of sequestration. Additionally, in the past, this analyst invested his own time and money to obtain cyber training. According to an ICE official, he has received more training requests than funds available, and the component is not compliant with its policy requirement for agents to receive 120 training hours in a 3-year period.⁷

Both ICE and USSS personnel expressed that there are very few formal training opportunities for non-technical operators and agents; rather, components have placed more emphasis on training forensics personnel. Due to the high costs

⁶ Under Secretary of Management's *Cybersecurity Workforce Management Support*, Directive 140-02, May 2013.

⁷ Homeland Security Investigations, *Computer Forensics Handbook*, HIS HB-11-01, April 2011.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

associated with the training, many cyber analysts are required to obtain free training. At times, DHS personnel are placed on a waiting list for free training offered by the Department of Defense Cyber Crime Center, as priority is given to the Department of Defense employees or military personnel.

Our interviews of selected cyber analysts and agents indicated that DHS would benefit from establishing a department-wide training program for ICE, NPPD, and USSS personnel to obtain common skill sets, attain professional certifications, promote knowledge sharing, and strengthen working relationships. In addition, interviewees indicated that group training would be more cost-effective if components coordinated their training development efforts. According to the Executive Director, DHS has drafted a comprehensive list of foundational and specialized cyber courses, but some of the training courses will not be available until the summer of 2016.

Without developing the department-wide training program, component personnel may not possess the skills necessary to perform their assigned incident response duties or investigative responsibilities in the event of a cyber attack. It may be difficult also for ICE, NPPD, and USSS personnel to obtain the necessary knowledge to address, mitigate, and investigate evolving cyber threats. Establishing a comprehensive training program would allow DHS to effectively perform its cyberspace mission and ensure that its personnel progress in their careers. Further, a coordinated training program may reduce the overall costs and redundancy of cyber courses across the Department.

Recommendation

We recommend that the Principal Deputy Assistant Secretary for Cyber Policy:

Recommendation 2. Coordinate with the DHS Chief Human Capital Officer to develop the department-wide trainings for cyber analysts and special agents to perform their duties.

DHS Comments to Recommendation 2

DHS concurred with recommendation 2. In fact, in recent years, the DHS Office of Chief Human Capital Officer's (CHCO) CyberSkills Management Support Initiative (CMSI) has worked with cybersecurity programs across DHS components to gather cybersecurity training requirements and catalog existing cybersecurity training programs. CMSI has compiled data about component-specific training needs, including information about skills required for position success and the learning objectives most critical to effective training for certain positions. CMSI has worked with technical experts across the components to review the collected data and draft a comprehensive cybersecurity training curriculum. The draft curriculum covers training from



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

the baseline through the superior proficiency level. In addition, the draft curriculum includes recommendations for general indoctrination training of all DHS cybersecurity employees through customized courses intended to refine the technical skills of Department's most proficient cybersecurity operators.

Relatedly, the NPPD has coordinated with CHCO regarding NCCIC training plan development and efforts since November 2014. Specifically, NCCIC has developed a training plan that meets the unique needs and requirements of the multiple NCCIC analyst types and ensures that these efforts can be leveraged by CHCO. NPPD will continue to work with CHCO to ensure that NPPD's efforts are aligned with the National Initiative for Cybersecurity Education, and that training materials and resources can be leveraged across the Department, as appropriate.

DHS agrees with the recommendation to develop department-wide training for cyber personnel and CHCO will work with CIR to review existing training requirements data and program proposals. CHCO and CIR also will review results of CMSI's ongoing efforts to review and validate mission critical cybersecurity positions for insights into possible refinements to training proposals. CHCO and CIR will then produce a department-wide training program implementation plan for DHS senior leadership approval and subsequent implementation. The estimated completion date is March 31, 2016.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS Components Would Benefit from an Enterprise-wide Automated Capability for Sharing Cyber Information

The Department does not have the capability to provide near real-time incident information that can enhance the coordinated response efforts among its components. Specifically, DHS does not have an enterprise-wide automated capability to share cyber threat and vulnerability information across the Department.

Currently, ICE, NPPD, and USSS use Treasury Enforcement Communications System, Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information, e-mail, phone, and personal interaction to



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

exchange cyber-related information.⁸ However, component personnel indicated that the current process has limited the analysts and investigators' abilities to develop a comprehensive picture of the incidents or correlations and trends among cyber attacks. For example, ICE and USSS agents cannot perform searches of the Treasury Enforcement Communications System to obtain information from other components regarding current cases or past investigations. Additionally, an ICE official informed us that the Structured Threat Information Expression/Trusted Automated Exchange of Indicator Information is currently a manual information sharing system, and the component must work with USSS to gather additional data as needed.

Senior officials from ICE, NPPD, and USSS acknowledged the need for a system that can integrate component data to provide a continuously updated, comprehensive picture of cyber threat and network status to support a coordinated incident response. However, such a system has not been established because the Department currently does not have the infrastructure to support an enterprise-wide system. In addition, such an automated system would need a network infrastructure separate from the one that supports the Department's normal operations.

The *Homeland Security Act of 2002* requires DHS to establish appropriate systems, processes, and procedures to share homeland security information relevant to threats and vulnerabilities with other Federal departments and agencies, state and local governments, and the private sector in a timely manner. According to the *Blueprint for a Secure Cyber Future*, components are required to improve threat information sharing and reduce incident response times through improved coordination and collaboration capabilities. Further, DHS must improve its automated capabilities to improve information sharing efficiencies across the Department.⁹

Without the enterprise-wide automated capability for real-time cyber data sharing, cyber analysts and special agents will continue to face obstacles when researching and sharing cyber information. For example, ICE, NPPD, and USSS may not have access to or receive the appropriate indicators and warning information to alert them of emerging threats to the Nation's cyber infrastructure. Moreover, in conjunction with improved understanding of others' cyber missions, an automated cyber capability would allow the

⁸ Structured Threat Information Expression is a computing language that enables organizations to share structured cyber threat information. Trusted Automated Exchange of Indicator Information is the main transport mechanism for sharing cyber threat information in a secure and automated manner.

⁹ *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise – DHS Cybersecurity Mission Management Plan*, May 2013.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

components to share actionable information to respond to and investigate incidents more timely.

Recommendation

We recommend that the Principal Deputy Assistant Secretary for Cyber Policy:

Recommendation 3. Collaborate with components to develop an incremental approach for acquiring the automated capability needed to share cyber information in real time across the Department.

DHS Comments to Recommendation 3

DHS concurred with recommendation 3. This action will be jointly led by the DHS Chief Information Officer and the Deputy Under Secretary for Cyber Security and Communications. Since the start of fieldwork, NPPD has put in place mechanisms for the NCCIC to share cyber threat information with the Federal network (.gov). While the focus is on sharing information for the purposes of network defense, NPPD is actively working with key DHS components, along with other agencies to develop the solution. With all components adopting the same standards (i.e., STIX/TAXII), DHS will be well positioned to integrate and enable automated information sharing.

In developing the information requirements to share indicators in near real time, NPPD has been working collaboratively with interagency partners such as the Federal Bureau of Investigation and the Intelligence Community, and other DHS components, including ICE, DHS Office of the Chief Information Officer, Civil Rights and Civil Liberties, Office of the General Counsel, Privacy Office, and USSS. Once developed, the aforementioned Cyber Strategy Implementation Plan also should inform requirements for an automated capability, including the data elements that can and will be shared, information handling procedures, and access controls. This capability will then be utilized to share cyber indicators more effectively across the DHS components. The estimated completion date is August 31, 2016.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will remain open until DHS provides documentation to support that all planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Technical Enhancements Could Strengthen Cyber Mission Information Systems

We identified vulnerabilities on internal websites at ICE and USSS that may allow unauthorized individuals to gain access to sensitive data. In addition, ICE has not implemented on its Windows workstations and servers all the DHS baseline configuration settings that are required to maintain an effective and standardized set of security controls.

Internal Website Vulnerabilities Exist

Security vulnerabilities exist on internal websites used by ICE and USSS agents to report investigation statistics, case tracking, and information sharing. For example, we identified:

- cross-frame scripting vulnerabilities at ICE and USSS. Successful exploitation of these vulnerabilities could allow an attacker to mislead a legitimate user to providing sensitive information, conduct privileged functions, or execute clickjacking attacks;
- reflected cross-site scripting vulnerabilities at ICE. If exploited, this may allow an attacker to hijack a user account, assist in worm propagation, and cause a denial of service attack;¹⁰
- a structured query language injection vulnerability at ICE. Exploitation of this vulnerability can lead to the modification of supporting infrastructure, such as a database;¹¹
- a file potentially containing sensitive information was unprotected on a USSS website. Viewing this file could give an unauthorized individual detailed system information about the web server that hosts the website; and
- a session fixation vulnerability on the USSS website that allows an attacker to impersonate a legitimate user.¹² Successful exploitation of this vulnerability may impact the Department's cyber data confidentiality and integrity.

¹⁰ Cross-frame and cross-site scripting are vulnerabilities that allow attackers to inject malicious code into an otherwise benign website. A clickjacking attack deceives the victim into interacting with user interface elements on the target website without user knowledge, executing privileged functionality on the victim's behalf. A worm is a type of malicious code that is a self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

¹¹ A structured query language injection attack occurs when code is inserted or "injected" into a user input box to execute a specific command.

¹² Session fixation is an attack that permits an attacker to hijack a valid user session.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ICE stated that its selected websites are not scanned with a vulnerability assessment tool. This limits the ability of ICE to identify and resolve website based weaknesses. ICE was unaware of the specific vulnerabilities our tool identified. USSS recently acquired a website assessment tool and was in the process of resolving identified issues at the time of our audit.

DHS requires components to manage systems to reduce vulnerabilities through testing, promptly installing patches, and eliminating or disabling unnecessary services. In addition, DHS requires components to conduct vulnerability assessments and/or testing to identify security weaknesses on information systems containing sensitive information annually.

Without remediating the vulnerabilities identified, sensitive cyber mission data may be compromised. Further, websites operating without the required configuration settings increases the risk that malicious users can circumvent the security controls that protect ICE and USSS systems.

ICE C3 System Security Controls Need Improvements

ICE has not implemented all the required DHS baseline configuration settings on its Cyber Crimes Center (C3) workstations and servers, which may allow sensitive data to be compromised. DHS established the required baseline configuration settings to provide the guidelines and parameters for ensuring a minimum baseline of security when installing or configuring operating systems. The guidelines include controls such as user access, password management, auditing, and computer services. When properly implemented, these settings help secure the confidentiality, integrity, and availability of the information and system.

However, our assessment revealed that ICE had only implemented 79 percent of the selected Windows 7 control settings outlined in the DHS baseline configuration guidance. Additionally, ICE implemented only 58 percent of the selected Windows 2008 server security control settings outlined in the DHS baseline configuration guidance.¹³ We assessed the effectiveness of controls implemented by interviewing selected information technology personnel, examining completed security control checklists, and conducting automated scans on selected workstations and servers for compliance with applicable DHS baseline configuration guidance.¹⁴ We identified the following configuration deficiencies that may be exploited if not addressed timely:

¹³ Subsequent to our testing, ICE updated selected controls for its Windows 2008 servers with the exception of renaming the local administrator account.

¹⁴ Baseline configuration settings provide system administrators with procedures that will ensure a minimum baseline of security in the installation and configuration of the hardware and software.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- The built-in local administrator account was not disabled on two workstations. DHS requires this account be disabled to reduce the possibility of brute force password guessing attacks.¹⁵
- The built-in local administrator account was not renamed on the workstations and servers. DHS requires this account is renamed to reduce the possibility of a brute force password guessing attack. Windows 7 desktop computers were configured to allow the usernames and passwords used for network authentication to be saved on local machines. DHS prohibits usernames and passwords from being saved on desktop computers to reduce the risk of a brute force attack.¹⁶
- The virtual memory pagefile on workstations and servers were not configured properly. An attacker who has physical access to the computers can view the information stored within the file. DHS requires this file be cleared to erase sensitive information during system shutdowns.
- Local server audit settings were not enabled to record user logons, account management, privileged use, and system events and did not comply with DHS Windows 2008 server guidance. DHS requires these events be recorded.

According to an ICE official, repeated turnover in the Information System Security Officer (ISSO) position contributed to noncompliance with the required baseline settings. For example, ICE has had six different ISSOs in the past 2½ years. The ICE official stated that the component just filled the C3 primary ISSO position in March 2015.

Without implementing the required configuration settings, ICE cannot ensure that its C3 workstations and servers are secured and protected from unauthorized access. Specifically, a compromised desktop could provide an unauthorized user with access to the C3 network. Implementing the required configuration settings will reduce the risk that sensitive information may be exposed.

Recommendations

We recommend that the ICE Chief Information Officer:

¹⁵ A brute force password attack is a method of accessing a device through attempting multiple combinations of numeric and/or alphanumeric passwords.

¹⁶ The username and password needed to authenticate a user are allowed to be stored on the desktop computer in the event the network connection is not available.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Recommendation 4. Mitigate identified website vulnerabilities or accept the risk by documenting the weaknesses in C3's system security plan.

Recommendation 5. Implement the required DHS sensitive systems configuration settings on Windows workstations and servers that support the C3, or accept the risk by documenting the deviations in the system security plan.

We recommend that the USSS Chief Information Officer:

Recommendation 6. Mitigate identified website vulnerabilities or accept the risk by documenting the weaknesses in the Criminal Investigative Division Suite's (CIDS) system security plan.

DHS Comments to Recommendation 4

DHS concurred with recommendation 4. ICE C3 will mitigate vulnerabilities identified during the scans. Moving forward, ICE will continue to use these best practices and audit findings as a guide to any updates or changes. Additionally, ICE C3 will create a hardened C3 workstation and server image pursuant to the *DHS 4300A DHS Sensitive System Policy* guidelines. The estimated completion date is November 30, 2015.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation 5

DHS concurred with recommendation 5. ICE C3 will mitigate vulnerabilities identified during the scans. Moving forward, ICE will continue to use best practices and audit findings as a guide to any updates or changes. Additionally, ICE C3 will create a hardened C3 workstation and server image pursuant to the DHS 4300A guidelines. The estimated completion date is November 30, 2015.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation 6

DHS concurred with recommendation 6. Mitigation of all the identified vulnerabilities has been completed. Noted technical vulnerabilities have been remediated, as evidenced by supporting documentation sent to the OIG on March 27, 2015. The USSS Chief Information Security Officer subsequently received acknowledgement and acceptance of remediation artifacts from the OIG. Given completion of the aforementioned actions, DHS requests that the OIG consider this recommendation resolved and closed.

OIG Analysis of DHS Comments

USSS Chief Information Security Officer provided us with supporting documentation for the hosting server. However, the assessment did not include the website application. This recommendation is unresolved and will remain open until vulnerabilities identified on the hosting server and website application are mitigated and supporting documentation is provided.

ICE and USSS Are Not Compliant with Certain DHS Information Security Program Requirements

ICE and USSS are not complying with all of the Department's information security program and *Federal Information Security Management Act* requirements. Specifically, USSS did not develop POA&Ms for its CIDS information system, as required. USSS also is not consistently updating the POA&Ms according to DHS policies. Further, we determined that ICE and USSS have not provided annual specialized training to individuals with significant security responsibilities.

POA&Ms

USSS has not properly maintained POA&Ms for its CIDS. POA&Ms are corrective action plans for tracking and planning the resolution of known information security weaknesses. Each POA&M must possess key data elements, such as weakness descriptions, creation dates, resources required, scheduled completion dates, changes to completion dates, weakness source, and status. POA&Ms provide management officials with a high-level view of what remediation actions are needed to correct the information security



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

weaknesses. Components are required to create POA&Ms to identify, track, and manage information security weaknesses.¹⁷

Our review of CIDS POA&Ms revealed that key information is missing, such as required resources, status, scheduled completion dates, and milestone information. According to a DHS Chief Information Security Office official, USSS is in the process of uploading its system POA&Ms, including security authorization documentation, into the Department's enterprise management system. Consequently, adequate POA&Ms have not yet been developed for all USSS systems. As a result, DHS' March 2015 information security scorecard indicated that USSS received a failing score for the weakness remediation (26 percent) metric. The DHS Chief Information Security Office expects USSS to improve its POA&M weakness remediation by the third quarter of fiscal year 2015.

Without properly maintained POA&Ms, USSS cannot identify, assess, prioritize, and monitor security weaknesses related to its programs and information systems. Further, when POA&Ms are not developed for known information technology security weaknesses, authorizing officials do not have the most accurate information to make credible, risk-based decisions regarding the security posture of the system.

Specialized Security Training

ICE and USSS have not provided annual, specialized security training required for individuals with significant security responsibilities. For example, the system administrator for C3 and the Child Exploitation Tracking System (CETS) did not receive the annual specialized security training in 2014. Further, we determined that USSS had not provided specialized training to CIDS' ISSO and assistant ISSO in 2014. USSS management did not provide any justification for not satisfying the specialized training requirement.

DHS requires personnel and contractors with significant security responsibilities to receive specialized training annually. The training is designed to inform personnel about the risks associated with their activities when accessing Federal information systems and their responsibilities in complying with DHS policies and procedures designed to reduce these risks.

When the required specialized training is not provided, components cannot ensure that their personnel with significant security responsibilities have the appropriate skills and knowledge to properly administer and secure systems

¹⁷ *DHS Sensitive Systems Handbook Directive 4300A, Attachment H, Process Guide for Plan of Action and Milestones*, version 11.0, December 3, 2014.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

against potential attacks. In addition, annual specialized training will enhance staff's understanding and readiness regarding emerging security issues, reporting requirements, and appropriate mitigation strategies.

Recommendations

We recommend that the ICE Executive Associate Director of Homeland Security Investigations:

Recommendation 7. Provide annual specialized or role-based training to personnel with significant security responsibilities to ensure that C3 and CETS are properly secured and managed.

We recommend that the USSS, Assistant Director, Office of Investigations:

Recommendation 8. Create, update, and maintain POA&Ms for all known information technology security weaknesses for CIDS in accordance with DHS guidance.

Recommendation 9. Provide annual specialized training to personnel with significant security responsibilities to ensure that CIDS is properly secured and managed.

DHS Comments to Recommendation 7

DHS concurred with recommendation 7. ICE will ensure that all C3 personnel with significant information technology security responsibilities leverage any/all applicable Virtual University training opportunities related to information system security. The estimated completion date is November 30, 2015.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS Comments to Recommendation 8

DHS concurred with recommendation 8. USSS will create, update, and maintain POA&Ms for all known information technology security weaknesses for CIDS; however, currently there are no known information technology security weaknesses in CIDS. Therefore, DHS requests that the OIG consider this recommendation resolved and closed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis of DHS Comments

As of February 2015, USSS had created several POA&Ms that are missing key information for known CIDS information technology security weaknesses. This recommendation is unresolved and will remain open until USSS provides supporting documentation showing all key information and POA&Ms are completed.

DHS Comments to Recommendation 9

DHS concurred with recommendation 9. USSS has instituted a training plan for personnel with significant security responsibilities related to CIDS. USSS will utilize DHS Headquarters-provided training and keep certificates of completion on file. Principals supporting CIDS will take the following training: Information Systems Security Officer- Information Technology Security Awareness, Phishing, Privacy-Protecting Personal Information, System Administrator and Privileged User, and System Owner training. The estimated completion date is August 31, 2015.

OIG Analysis of DHS Comments

We agree that the steps DHS has taken satisfy the intent of this recommendation. We consider this recommendation resolved, and it will remain open until DHS provides documentation to support that all planned corrective actions are completed.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

The objectives of our audit were to determine whether DHS (1) had delineated the roles and responsibilities among component's cyber missions, and (2) established a process to promote department-wide information sharing and coordinated response efforts for cyber incidents and criminal activities. Additionally, we assessed the effectiveness of security controls implemented to protect data collected, processed, and generated by selected systems; and determined whether component information systems used to exchange cyber data were in compliance with DHS information security program requirements.

Our audit focused on the requirements, recommendations, and goals outlined in the following key documents:

- Deputy Secretary's *Strengthening Departmental Unity of Effort in Cyber Security* (November 2014),
- Presidential Executive Order 13636 - *Improving Critical Infrastructure Cybersecurity* (February 2013),
- *Blueprint for a Secure Cyber Future* (November 2011),
- *Federal Information Security Modernization Act of 2014* (December 2014),
- *DHS Sensitive Systems Policy Directive 4300A* (April 2014),
- DHS Sensitive Systems Configuration Guidance.

We also consulted other relevant guidance published by OMB and the National Institute of Standards and Technology.

To conduct our audit, we interviewed selected ICE, DHS Management, NPPD, Office of Policy, and USSS officials. We evaluated information sharing policies, standard operating procedures, training records, and system security documentation for selected systems. Finally, we evaluated the effectiveness of security controls implemented to protect the data collected, processed, and generated by selected systems that support ICE and USSS' cyber missions.

As part of this audit, we also evaluated ICE and USSS' compliance with applicable DHS information security program requirements on selected



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

systems used by ICE and USSS to perform their cyber missions. Specifically, we evaluated:

- ICE C3 System - used to investigate large-scale producers and distributors of child pornography, as well as individuals who travel abroad for the purpose of Child Sex Tourism.
- ICE CETS – serves as a centralized information repository that assists law enforcement in conducting child exploitation investigations and aggregates tips and lead information about Internet-facilitated child sexual exploitation crimes.
- USSS CIDS- is a collection of criminal investigative tools used by the Criminal Investigative Division for investigation into financial crimes.

We performed our field work in the Washington, DC, area. Technical security assessments were not performed at NPPD.¹⁸

We conducted this performance audit between December 2014 and April 2015 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in appendix C.

¹⁸ Technical security assessments were not performed on any NPPD systems as we have performed multiple audits at the component within the last 5 years, such as *Implementation Status of EINSTEIN 3 Accelerated* (OIG-14-52, March 2014); *DHS Can Take Actions to Address Its Additional Cybersecurity Responsibilities* (OIG-13-95, June 2013); *Planning, Management, and Systems Issues Hinder DHS' Efforts to Protect Cyberspace and the Nation's Cyber Infrastructure* (OIG-11-89, June 2011); and *DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems* (OIG-10-111, August 2010).



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B

DHS Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

August 6, 2015

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Office of Information Technology Audits

FROM: Jim H. Crumacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office 

SUBJECT: Management's Response to OIG Draft Report: "DHS Can
Strengthen Its Cyber Mission Coordination Efforts"
(Project No. 15-013-ITA-ICE)

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS is pleased with OIG's recognition that the Operational and Headquarters Components have strengthened coordination in performing their cyber missions, particularly with respect to sharing information associated with investigating and responding to cyber attacks. The draft report aptly states that cyberspace is critical to both the economic prosperity and security of the nation. Though constantly challenged to preserve and protect it for the homeland, and in spite of recent high-profile cyber attacks on federal agencies and major private sector corporations, DHS remains front and center in the national effort to protect, prevent, mitigate, respond to and recover from cyber incidents.

Beginning with the 2011 "Blueprint for a Secure Cyber Future," and continuing with the 2013 "National Infrastructure Protection Plan," the 2014 "Quadrennial Homeland Security Review," and the "Fiscal Years (FYs) 2014-2018 Strategic Plan," DHS has taken progressively stronger steps to safeguard cyberspace and align the Department's cyber capabilities for this critical mission. Very early in their DHS tenures, Secretary of Homeland Security Jeh Johnson and Deputy Secretary Alejandro Mayorkas placed great emphasis and urgency on the cyber mission and have aggressively marshalled the Department's policies, resources and structure to assure its sustained relevance and viability.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Emblematic of their commitment to this effort was the Deputy's memorandum to DHS leadership, "Strengthening Departmental Unity of Effort in Cyber Security," dated November 12, 2014, which applied the Secretary's Unity of Effort principles to this mission and decreased risk in prioritized focus areas. Moreover, their efforts continue with the soon to be released DHS 2015 "Cyber Strategy," which when approved and implemented will reinforce existing cyber security missions and develop the use of cyber capabilities and techniques, as enablers for the Department's other homeland security missions. These actions, when amplified by the Department's cyber initiatives and accomplishments since the OIG's fieldwork ended (described in the individual responses below), demonstrate that DHS is, in fact, on course to further enhance its cyber mission coordination efforts.

The draft report contained nine recommendations with which the Department concurs. Specifically:

Recommendation 1: That the Principal Deputy Assistant Secretary for Cyber Policy develop a comprehensive, cross-departmental strategic implementation plan that defines components' cyber missions and responsibilities, including long-term goals, performance metrics, and milestones to measure progress in unifying the Department's incident response and coordination efforts.

Response: Concur. Although the report correctly indicates that the "Office of Policy-Cyber has not developed a cyber strategic implementation plan due to its recent establishment and limited staff," it is worth noting that the "DHS FY 2014-2018 Strategic Plan" signed Secretary Johnson on December 7, 2014, does establish Mission 4 (Safeguard and Secure Cyberspace). Moreover, following Office of Management and Budget Circular A-11, "Preparation, Submission, and Execution of the Budget" guidance and consistent with the "GPRA Modernization Act of 2010 (P.L. 111-352)," pages 29-34 of the strategic plan prescribe goals, performance metrics and planned targets associated with that mission for the Department.

Additionally, since the start of fieldwork associated with this audit, the DHS Office of Policy (PLCY) [the Cyber, Infrastructure & Resilience Policy (CIR) and Strategy, Planning, Analysis & Risk (SPAR) Divisions] teamed to build the "DHS 2015 Cyber Strategy." This strategy has been vetted among Component and Headquarters, and was submitted to the DHS senior leadership in July 2015 for approval and signature. The draft mandates development of a "Cyber Strategy Implementation Plan" within 90 days of the strategy's approval. The Implementation Plan will specify strategic objectives, corresponding tasks, and associated performance metrics.

The strategy also directs the establishment of a Cyber Strategy Implementation Group (CSIG) within 30 days, and the stand up of a formal Cyber Advisory Board (CAB) within 60 days. In the aggregate, the "FY 2014-2018 Strategic Plan" and the "2015 Cyber



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Strategy's Implementation Plan" will satisfy requirements for a cross-departmental strategic implementation plan. The Acting Assistant Secretary for CIR Policy will chair the CSIG and oversee both the development and execution of the Implementation Plan. Estimated Completion Date (ECD): February 29, 2016.

Recommendation 2: That the Principal Deputy Assistant Secretary for Cyber Policy coordinate with the DHS Chief Human Capital Resource Officer to develop the Department-wide training for cyber analysts and special agents to perform their duties.

Response: Concur. In fact, in recent years the DHS Office of the Chief Human Capital Officer's (CHCO) CyberSkills Management Support Initiative (CMSI) has worked with cybersecurity programs across DHS Components to gather cybersecurity training requirements and catalog existing cybersecurity training programs. CMSI has compiled data about component-specific training needs, including information about skills required for position success and the learning objectives most critical to effective training for certain positions. CMSI worked with technical experts across the Components to review the collected data and draft a comprehensive cybersecurity training curriculum. The draft curriculum covers training from the baseline through the superior proficiency level; therefore, it includes recommendations for general indoctrination training of all DHS cybersecurity employees through custom training courses intended to refine the technical skills of Department's most proficient cybersecurity operators.

Relatedly, the National Protection and Programs Directorate (NPPD) has coordinated with DHS CHCO regarding National Cybersecurity and Communications Integration Center (NCCIC) training plan development and efforts since November 2014. Specifically, NCCIC has developed a training plan that meets the unique needs and requirements of the multiple NCCIC analyst types and ensures that these efforts can be leveraged by DHS CHCO. NPPD will continue to work with DHS CHCO to ensure that NPPD efforts are aligned with the National Initiative for Cybersecurity Education, and that training materials and resources can be leveraged across the Department, as appropriate.

DHS agrees with the recommendation to develop Department-wide training for cyber personnel and CHCO will work with CIR to review existing training requirements data and program proposals. CHCO and CIR will also review results of the CMST's ongoing effort to review and validate mission critical cybersecurity positions for insights into possible refinements to training proposals. CHCO and CIR will then produce a Department-wide training program implementation plan for DHS senior leadership approval and subsequent implementation. ECD: March 31, 2016.

Recommendation 3: That the Principal Deputy Assistant Secretary for Cyber Policy collaborate with components to develop an incremental approach for acquiring the automated capability needed to share cyber information real time across the Department.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Response: Concur. This action will be jointly led by the DHS Chief Information Officer and the Deputy Under Secretary for Cyber Security and Communications. Since the start of fieldwork, NPPD has put in place components for the NCCIC to share cyber threat information with the .gov. While the focus is on sharing with the .gov for purposes of network defense, NPPD is actively working with key DIIS Components along with the interagency to develop the solution. With all department components adopting the same standards (i.e., STIX/TAXII¹), DHS will be well positioned to integrate and enable automated information sharing.

In developing the information requirements to be able to share indicators in near real time, NPPD has been working collaboratively with interagency partners such as the Federal Bureau of Investigation and Intelligence Community, and other DHS components, including the United States Secret Service (USSS), Immigration and Customs Enforcement (ICE), DHS Office of the Chief Information Officer, Privacy Office, Civil Rights and Civil Liberties, and Office of the General Counsel. Once developed, the aforementioned Cyber Strategy Implementation Plan should also inform requirements for an automated capability to include: the data elements that can and will be shared, information handling procedures, and access controls. This capability will then be utilized to share cyber indicators more effectively across all DHS components. ECD: August 31, 2016.

Recommendation 4: That the ICE Chief Information Officer mitigate identified website vulnerabilities or accept the risk by documenting the weaknesses in C3's system security plan.

Response: Concur. ICE C3 will mitigate identified vulnerabilities identified during the scans. Moving forward, ICE will continue to use these best practices and audit finding as a guide to any updates or changes. Additionally, ICE C3 will create a hardened C3 workstation and server image pursuant to the DHS 4300a "DHS Sensitive System Policy" guidelines. ECD: November 30, 2015.

Recommendation 5: That the ICE Chief Information Officer implement the required DHS sensitive systems configuration settings on Windows workstations and servers that support the C3, or accept the risk by documenting the deviations in the system security plan.

Response: Concur. ICE C3 will mitigate identified vulnerabilities identified during the scans. Moving forward, ICE will continue to use these best practices and audit finding as a guide to any updates or changes. Additionally, ICE C3 will create a hardened C3

¹ Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

workstation and server image pursuant to the DHS 4300a guidelines. ECD: November 30, 2015.

Recommendation 6: That the USSS Chief Information Officer mitigate identified website vulnerabilities or accept the risk by documenting the weaknesses in the Criminal Investigative Division Suite's (CIDS) system security plan.

Response: Concur. Mitigation of all the identified vulnerabilities has been completed. Noted technical vulnerabilities have been remediated as evidenced by supporting documentation sent to OIG on March 27, 2015. The USSS Chief Information Security Officer subsequently received acknowledgement and acceptance of remediation artifacts from OIG. Given completion of the aforementioned actions, DHS requests that OIG consider this recommendation resolved and closed.

Recommendation 7: That the ICE Executive Associate Director of Homeland Security Investigations provide annual specialized or role-based training to personnel with significant security responsibilities to ensure that C3 and CETS are properly secured and managed.

Response: Concur. ICE C3 will ensure all personnel with significant Information Technology (IT) security responsibilities take any/all applicable Virtual University training opportunities related to information system security. ECD: November 30, 2015.

Recommendation 8: That the USSS, Assistant Director, Office of Investigations create, update, and maintain POA&Ms for all known IT security weaknesses for CIDS in accordance with DHS guidance.

Response: Concur. USSS will create, update, and maintain POA&Ms for all known IT security weaknesses for CIDS; however currently there are no known IT security weaknesses in CIDS. Therefore, DHS requests that OIG consider this recommendation resolved and closed.

Recommendation 9: That the USSS, Assistant Director, Office of Investigations provide annual specialized training to personnel with significant security responsibilities to ensure that CIDS is properly secured and managed.

Response: Concur. USSS has instituted a training plan for personnel with significant security responsibilities related to CIDS. USSS will utilize DHS HQ provided training and keep certificates of completion on file. Principals supporting CIDS will take the following training: ISSO- IT Security Awareness, Phishing, Privacy- Protecting Personal Information, System Admin- System Administrator and Privileged User, and System Owner- System Owner training. ECD: August 31, 2015.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C

**Office of Information Technology Audits Major Contributors to
This Report**

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Shannon Frenyea, Team Lead
Aaron Zappone, Team Lead
Tom Rohrback, IT Specialist
Tonya McKinnon, IT Auditor
Jason Dominguez, Referencer



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix D

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Chief Information Officer (CIO)
Chief Information Security Officer
CIO, ICE
CIO, USSS
Executive Associate Director of Homeland Security Investigations, ICE
Deputy Under Secretary, Office of Cybersecurity and Communications, NPPD
Acting Assistant Secretary for Cyber, Infrastructure, and Resilience, PLCY
Assistant Director, Office of Investigations, USSS
Audit Liaison, USSS
Audit Liaison, NPPD
Audit Liaison, ICE

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

ADDITIONAL INFORMATION AND COPIES

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov. Follow us on Twitter at: @dhsoig.



OIG HOTLINE

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive, SW
Washington, DC 20528-0305