OFFICE OF INSPECTOR GENERAL

Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015

Homeland Security

November 1, 2017
OIG-18-10

DHS OIG HIGHLIGHTS

Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015

November 1, 2017

Why We Did This Review

Section 107 of the *Cybersecurity Act of 2015* requires the Inspectors General from the Intelligence Community and the Departments of Commerce, Defense, Energy, Justice, Homeland Security, and Treasury to submit a joint report to the Congress on the actions the Federal Government has taken to share cybersecurity information. We evaluated the Department of Homeland Security's progress in meeting its cybersecurity information sharing requirements.

What We Recommend

We recommend NPPD improve its information sharing capability by acquiring technologies needed for cross-domain sharing and automated analysis of cyber threat data, enhancing outreach to promote DHS' information sharing program, and implementing required security controls on selected information systems.

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

The Department has addressed information sharing requirements of Title I, Section 107 of the *Cybersecurity Act of 2015*. Specifically, DHS has developed adequate policies and procedures and the capability to share cyber threat indicators and defensive measures. Additionally, DHS has properly classified the indicators and defensive measures and accounted for the security clearances of private sector recipients of this shared information. Like some Federal agencies, DHS has used cyber threat indicator and defensive measures to mitigate potential threats.

Despite meeting these requirements, the Department faces challenges to effectively sharing cyber threat information across Federal and private sector entities. Given that NPPD emphasizes timeliness, velocity, and volume in cybersecurity information sharing, the system DHS currently uses does not provide the quality, contextual data needed to effectively defend against ever-evolving threats. Without acquiring a cross-domain information processing solution and automated tools, DHS cannot analyze and share threat information timely. Further, without enhanced outreach, DHS cannot increase participation and improve coordination of information sharing across Federal and private organizations.

As part of our review, we also determined that NPPD can improve the security of DHS component systems used to process and store cyber threat information by implementing required configuration settings and applying security patches more timely. Such actions are fundamental to securing the confidentiality, integrity, and availability of sensitive systems and the data they process.

Agency Response

NPPD concurred with all five recommendations and has implemented corrective actions to address the findings.

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

November 1, 2017

MEMORANDUM FOR: Jeanette Manfra
Assistant Secretary for Cybersecurity and Communications
National Protection and Programs Directorate

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

SUBJECT: *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*

Attached for your action is our final report, *Biennial Report on DHS' Implementation of the Cybersecurity Act of 2015*. We incorporated your comments in our report.

The report contains five recommendations aimed at enhancing the program's overall effectiveness. The Department concurred with all five recommendations. Based on information provided in your response to the draft report, we consider recommendations 4 and 5 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 supporting documentation necessary to inform us about the current status of the recommendation. 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 2 and 3 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. Recommendation 1 is closed. Please send your response or closure request to OIGAuditsFollowup@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

Table of Contents

Appendixes

Abbreviations

AIS	Automated Indicator Sharing
CISCP	Cyber Information Sharing and Collaboration Program
CS&C	Office of Cybersecurity and Communications
ICE	United States Immigration and Customs Enforcement
IC IG	Office of the Inspector General of the Intelligence Community
MOE	Mission Operating Environment
NCCIC	National Cybersecurity and Communications Integration Center
NPPD	National Protection and Programs Directorate
OIG	Office of Inspector General
PII	personally identifiable information
SECIR	Stakeholder Engagement and Cyber Infrastructure Resilience
TLP	Traffic Light Protocol
TS	Top Secret
US-CERT	United States-Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

Background

On December 18, 2015, the President enacted the *Cybersecurity Act of 2015* (Cybersecurity Act) to establish a voluntary process for sharing cyber threat information between Federal and private sector entities.[1] The Act requires the Director of National Intelligence, the Secretaries of Defense and Homeland Security, and the Attorney General to develop and issue procedures jointly to facilitate and promote the sharing of classified and unclassified cyber threat indicators, defensive measures, and best practices to mitigate cyber threats. The Act encourages Federal and private organizations to share this information while protecting classified information, intelligence sources and methods, and privacy and civil liberties. According to the Cybersecurity Act, cyber threat indicators mean information that is necessary to describe or identify as:

- malicious reconnaissance, including anomalous patterns of communications, to gather technical information related to a cybersecurity threat or security vulnerability;
- methods of defeating a security control or exploitation of a security vulnerability;
- security vulnerabilities, including anomalous activity, that appear to indicate the existence of a security vulnerability;
- methods of exploiting a security vulnerability to gain unauthorized access to information or an information system,
- malicious cyber command and control;
- actual or potential harm caused as a result of a particular cybersecurity threat; and
- disclosure of any other attribute of a cybersecurity threat that is not prohibited by law.

Further, defensive measures are defined as actions, devices, procedures, signatures, techniques, or other measures applied to an information system to detect, prevent, or mitigate known or suspected cybersecurity threats or security vulnerabilities. However, these measures do not include actions to cause destruction, gain unauthorized access, or inflict substantial harm to an information system or information that is not owned by the private entity operating the measure, or other entity that is authorized to provide consent and has provided consent to that private entity for operation of such a measure.

In addition to the Cybersecurity Act, the *Homeland Security Act of 2012* requires DHS to establish appropriate systems, mechanisms, and procedures for sharing information relevant to threats and vulnerabilities in national

[1] Federal entities include Federal departments, agencies, and components of agencies.

critical infrastructure and key resources with other Federal agencies, state and local governments, and the private sector in a timely manner. Executive Order 13636 requires DHS to increase the volume, timeliness, and quality of cyber threat information sharing to secure the Nation's critical infrastructure, and promote cybersecurity through a technology-neutral framework.

DHS' Cyber Mission Responsibilities

DHS coordinates the national response to cyber incidents, such as the use of phishing, malicious software, identity theft, access device and bank fraud, and cyber intrusions.[2] The following components are actively involved in fulfilling the Department's cybersecurity mission:

- The National Protection and Programs Directorate (NPPD) protects and enhances the resilience of the Nation's physical and cyber infrastructure. The National Cybersecurity and Communications Integration Center (NCCIC), which is a division of the Office of Cybersecurity and Communications (CS&C) under NPPD, serves as the Federal Government's 24/7 hub for sharing cybersecurity information, providing technical assistance, and responding to security incidents.

- United States Immigration and Customs Enforcement (ICE) enforces Federal laws governing border control, customs, trade, and immigration to support homeland security and public safety. Homeland Security Investigations, an operational directorate of ICE, investigates all types of cross-border criminal activity including financial crimes, commercial fraud, cybercrimes, human rights, transnational gangs, and illegal immigration.

- United States Secret Service (Secret Service) safeguards the Nation's financial infrastructure and payment systems to preserve the integrity of the economy, and to protect national leaders, visiting heads of state and government, designated sites, and national special security events. To achieve its mission, the Secret Service conducts investigations to identify, locate, and apprehend criminal organizations and individuals targeting the Nation's critical infrastructure.

Cybersecurity Act Reporting Requirements

Title I, Section 107 of the *Cybersecurity Act of 2015* requires the Inspectors General from the Intelligence Community and the Departments of Commerce,

[2] 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.

Defense, Energy, Justice, Homeland Security, and Treasury to submit a joint report to appropriate congressional oversight committees, beginning in December 2017, and biennially thereafter. Specifically, the joint report shall include an overall assessment of:

- the policies, procedures, and guidelines to share cyber threat indicators within the Federal Government, including the removal of personal information that is not directly related to cyber threat indicators;

- whether cyber threat indicators or defensive measures have been properly classified and there is an accounting of the number of security clearances granted to private sector users to receive classified information under this Act;

- actions taken by the Federal agencies based on the cyber threat indicators or defensive measures shared within the Federal Government; and

- any barriers to sharing cyber threat indicators or defensive measures among Federal agencies.

In addition, the joint report submitted under this section of the Cybersecurity Act may include Inspector Generals' recommendations to improve or modify the authorities and processes under this title. We developed this separate, agency-level report based on our evaluation of DHS' progress in meeting its cybersecurity information sharing requirements. The objective, scope, and methodology for our report are included in appendix A.

According to the Office of the Inspector General of the Intelligence Community (IC IG) reporting instruction, each Office of Inspector General (OIG) of the selected agencies is required to submit responses to 11 questions on the actions DHS has taken to implement the Act. Our responses to these questions can be found in appendix C.

Results of Review

The Department has addressed the information sharing requirements of Title I, Section 105 of the *Cybersecurity Act of 2015*. Specifically, DHS has developed adequate policies and procedures and the capability to share cyber threat indicators and defensive measures. Additionally, DHS has properly classified the indicators and defensive measures and accounted for the security clearances of private sector recipients of this shared information. Like some Federal agencies, DHS has used cyber threat indicator and defensive measures to mitigate potential threats.

Despite meeting these requirements, the Department faces challenges to effectively sharing cyber threat information across Federal and private sector entities. Given that NPPD emphasizes timeliness, velocity, and volume in cybersecurity information sharing, the system DHS currently uses does not provide the quality, contextual data needed to effectively defend against ever-evolving threats. Without acquiring a cross-domain information processing solution and automated tools, DHS cannot analyze and share threat information timely. Further, without enhanced outreach, DHS cannot increase participation and improve coordination of information sharing across Federal and private organizations.

As part of our review, we also determined that NPPD can improve the security of DHS component systems used to process and store cyber threat information by implementing required configuration settings and applying security patches more timely. Such actions are fundamental to securing the confidentiality, integrity, and availability of sensitive systems and the data they process.

DHS Has Addressed Requirements of the Cybersecurity Act

We found that the Department has adequately addressed the following requirements of Title I, Section 107 of the Cybersecurity Act:

- developed adequate policies and procedures and a supporting capability to share cyber threat indicators and defensive measures;

- properly classified cyber threat indicators and defensive measures and accounted for the security clearances of private sector users authorized to receive this information; and

- used the cyber threat indicator and defensive measure information received to mitigate potential security risks.

Such actions are fundamental to DHS establishing a viable cyber threat information sharing capability with its Federal and private sector partners. These actions help ensure the program is dynamic and can grow or evolve over time in identifying useful information available through various data sources. Effective DHS coordination with other Federal entities can help ensure that the cyber threat information shared is timely, actionable, and unique.

Policies and Procedures for Sharing Cyber Threat Indicators

As required, DHS has implemented adequate policies and procedures needed for sharing cyber threat indicators and defensive measures with Federal and

private entities. In February 2016, the Office of the Director of National Intelligence, Departments of Defense, Homeland Security, and Justice jointly issued *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government* in accordance with the Act. The guidance requires Federal entities to establish and maintain procedures and implement protocols that facilitate and promote the sharing of cybersecurity information by the Federal Government in a timely manner. It encourages the Federal Government to share classified and unclassified cyber threat indicators and defensive measures with both Federal and private entities as broadly and as quickly as possible. In addition, the guidance describes mechanisms through which the appropriate Federal entities can share information with the private sector.

For example, the guidance provides examples of current procedures to support timely sharing of classified cyber threat information and defensive measures via the following.

- DHS' Enhanced Cybersecurity Services is part of DHS' overall efforts to protect U.S.-based companies' information systems and networks from intrusions, disruptions, and data exploitation. Enhanced Cybersecurity Services consists of the operational processes and security oversight required to share unclassified and classified cyber threat indicators with commercial service providers. The purpose of the program is to enhance the cybersecurity posture of participating commercial service providers by augmenting, not replacing, their current cybersecurity capabilities.

- DHS' Cyber Information Sharing and Collaboration Program (CISCP) is a program for public-private information sharing and complements ongoing DHS information sharing efforts. DHS and participating companies share information about cyber threats, incidents, and vulnerabilities. Information shared via CISCP allows all participants to better secure their own networks and helps support the shared security of CISCP partners.

- The Defense Industrial Based Cybersecurity Program is a Department of Defense program for sharing cyber threat information in order to enhance the overall security of unclassified defense industrial base networks, reduce damage to critical programs, and increase the Department's cyber situational awareness.

- The Department of Energy's Cybersecurity Risk Information Sharing Program is a public-private sector partnership that provides critical infrastructure operators with the ability to share cyber threat data and analytics, and receive automated mitigation measures in real time.

- The National Cyber Investigative Joint Task Force is a presidentially-mandated multi-agency center that coordinates, integrates, and shares threat information including classified indicators related to cyber investigations and operations.

Federal entities are encouraged to downgrade or declassify cyber threat information to ensure the information is disseminated to the largest audience and maximum extent possible.

Further, in June 2016, DHS helped the Department of Justice develop the following policies and procedures for exchanging cyber threat indicators and defense measures with private sector entities:

- *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015* - The guidance addresses identification of cyber threat indicators and defensive measures, dissemination of cybersecurity information, and protections for sharing information in accordance with the Cybersecurity Act.

- *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government* - The procedures describe the automated processes for receiving, handling, and disseminating information. They also provide guidelines for non-Federal entities to protect privacy and civil liberties within the timeframe stipulated in the Cybersecurity Act.

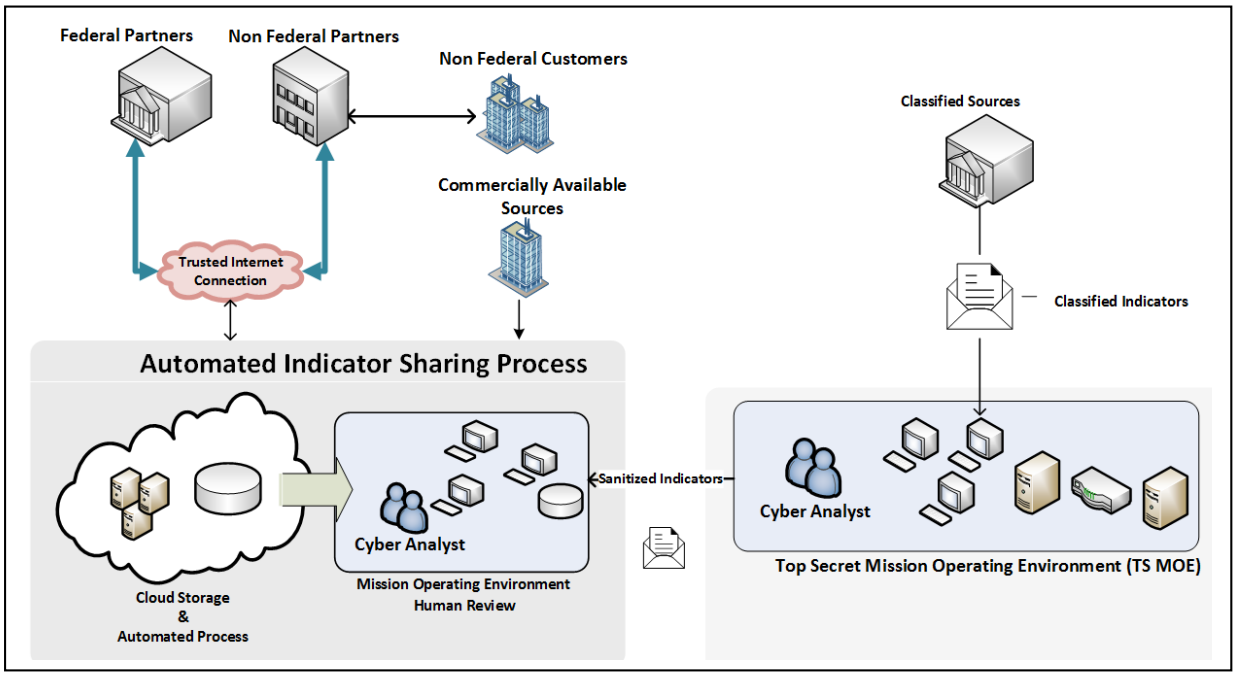
The Automated Indicator Sharing Program

To meet requirements of the Cybersecurity Act, DHS has implemented the Automated Indicator Sharing (AIS) program, with the goal of sharing cyber threat indicators and defensive measures in real time. The AIS program consists of information producers and consumers that exchange cyber threat indicators across the Federal Government and the private sector. Specifically, AIS participants are Federal departments and agencies; state, local, tribal, and territorial governments; private sector entities; information sharing and analysis centers and organizations; and foreign government companies. Federal entities exchange classified and unclassified cyber information in real time under the *Enhanced Shared Situational Awareness Multilateral Information Sharing Agreement.*[3]

[3] A Federal multi-agency agreement developed to enhance cybersecurity information sharing among Federal agencies to better protect the United States computer systems from malicious cyber threats fully consistent with the Federal laws and oversight requirements.

A supporting AIS automated capability allows DHS to exchange cyber threat information from different sources (e.g., commercially-available threat information, NPPD's cyber programs and indicator feeds, and partner-submitted data). Specifically, the NCCIC receives the cyber threat indicators and defensive measures submitted through AIS, removes personally identifiable information (PII) and other sensitive information that is not directly related to a cybersecurity threat, and disseminates the edited information to AIS participants, as appropriate. Cyber analysts use unclassified Mission Operating Environment (MOE) workstations to review the information received. The Top Secret (TS) MOE, a component of EINSTEIN 3 Accelerated, processes classified information for National Cybersecurity Protection System.[4] NPPD receives classified indicators via email. After classified information is removed, cyber analysts enter some of the declassified indicators into MOE to share with Federal and private sector partners. However, the background information supporting the now unclassified indicators may remain classified. The unclassified and classified data flows are illustrated in figure 1.

Figure 1: AIS and National Cybersecurity Protection System Cyber Threat Indicator Data Flow



Source: DHS OIG-generated based on information received from NPPD

[4] EINSTEIN consists of three versions: EINSTEIN 1, EINSTEIN 2, and EINSTEIN 3 Accelerated. Under EINSTEIN 1, NPPD deploys sensors on Federal agencies' external Internet connections to collect network flow records. EISTEIN 2 provides intrusion detection capability to issue alerts on potential malicious network activities. EINSTEIN 3 Accelerated combines existing analysis of Federal enterprise-wide EINSTEIN 1 and 2 data and commercial intrusion prevention services to counteract emerging threats.

As shown on the left side of figure 1, AIS participants share unclassified cyber threat information over a trusted (i.e., encrypted) Internet connection. The information is stored in the cloud or on machines and transferred to cyber analysts for review. Subsequently, the analysts send the machine-readable files to the AIS participants. AIS participants may analyze and manage the files with their own tools for their own purposes.

The right side of figure 1 shows how classified cyber threat indicators are sent to cyber analysts by email as there is no automatic transfer from TS MOE to MOE. Cyber analysts review and enter the classified indicators manually into TS MOE. The crosswalk shows that, after cyber analysts remove classified information from the indicators, the declassified indicators are entered into MOE by emails for sharing with Federal and non-Federal partners.

The Department shares unclassified cyber threat indicators and defensive measures through three data feeds:

- The AIS capability is for non-Federal entities that have signed the AIS Terms of Use, or are customers of AIS participants that are allowed to re-distribute the information.

- The CISCP distributes the cyber threat information to non-Federal entities that have signed the CISCP Cooperative Research and Development Agreement.

- FedGov shares cyber threat information with Federal departments and agencies that have signed the Multilateral Information Sharing Agreement.

DHS uses a Traffic Light Protocol (TLP) for cyber threat information sharing with non-Federal entities. TLP uses four colors (red, amber, green, and white) to designate the degree to which the information can be shared with recipients. Under TLP, the information source is responsible for ensuring that the recipients understand and follow the TLP sharing guidance. If a recipient needs to share the information more widely than indicated by the TLP designation, the recipient must obtain explicit permission from the original data source. According to NPPD and AIS business rules, TLP red cyber threat indicators are not shared through the AIS feed; this information is limited to those who participated in the specific exchange, meeting, or conversation in which it was originally disclosed. Table 1 depicts the TLP and sharing boundaries.

Table 1 – TLP Definitions and Boundaries

Color	When should it be used?	How may it be shared?
TLP:RED  Not for disclosure, restricted to participants only.	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER  Limited disclosure, restricted to participants' organizations.	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
TLP:GREEN  Limited disclosure, restricted to the community.	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.
TLP:WHITE  Disclosure is not limited.	Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Source: Table provided by NPPD U.S. Computer Emergency Readiness Team (US-CERT)

Classification of Cyber Threat Indicators and Accounting of Security Clearances Granted to Private Sector Users

As the Cybersecurity Act requires, DHS has properly classified cyber threat indicators and defensive measures. This was done primarily based on derivative classification and according to guidelines from other NPPD cybersecurity initiatives such as EINSTEIN and the Enhanced Cybersecurity Services program, used for information sharing. These guidelines provide instructions for classifying, reclassifying, and declassifying information and material under DHS purview. As of June 2017, DHS had issued 513,639 unclassified cyber threat indicators since it initially launched the AIS in March 2016. These indicators addressed a range of issues, such as malicious Internet protocol addresses, ransomware, phishing, and spam attacks. Further, from October 2015 to April 2017, the Department shared 2,290 classified cyber

threat indicators with the private sector to help mitigate potential cybersecurity incidents.

Under its original classification authority, DHS classified the majority of the cyber threat indicators it shared.[5] Nevertheless, in some instances, DHS may share classified cyber threat indicators and defensive measures using the derivative classification process. Under this process, DHS may develop a derivative classified document based on original classified material from another source. In such instances, DHS is required to apply the same classification level and markings to the derivative document as those on the original source document.

Further, DHS has adequately accounted for the security clearances of private sector entities with which it shares cyber threat information. According to the Cybersecurity Act, individuals within non-Federal entities must have the appropriate security clearances in order to receive classified cyber threat indicators and defensive measures. As of May 2017, DHS had granted 1,631 active security clearances to private sector individuals participating in the Department's various information sharing programs, including EINSTEIN and Enhanced Cybersecurity Services. DHS does not track the number of clearances issued for the purpose of sharing information under the AIS program alone.

Actions Taken by Federal Government Based on the Cyber Threat Indicators and Defensive Measures Shared

Using the DHS cyber threat indicators and defensive measures shared, Federal agencies have taken appropriate actions to protect their information systems and data. We interviewed representatives of selected DHS components and Federal entities—consumers of this information—and found that they generally used this information to improve their network security controls. However, they also used the cyber threat indicators to detect malicious actors, and mitigate anomalies and possible threats to their networks.[6] For example, we were told that, using the cyber indicators received, Secret Service was able to investigate and convict several cyber criminals for their role in cyberattacks committed against U.S. computer networks. One hacker was extradited from Italy to face charges in New Jersey for his participation in this international conspiracy to hack into networks to steal payment card data.

[5] Original classification (or original classifier) is the initial decision that particular information requires protection in the interest of national security and could be expected to cause damage if subject to unauthorized disclosure.

[6] We interviewed selected representatives from the Departments of Health and Human Services, State, Veterans Affairs, the National Aeronautics and Space Administration, and DHS components with cyber missions (ICE and Secret Service).

Some Federal agency representatives told us they share the cyber threat indicators and defensive measures received with critical infrastructure sectors, such as the Defense Industrial Base, Food and Agriculture, and Transportation. Further, a Department of State representative told us that State routinely shared the cyber and malware attack indicators it collected with DHS' Office of Intelligence and Analysis and the Department of Energy. State would either share original source information, or add details to the cyber threat information it had received from AIS or other sources to assist these agencies.

Challenges in Sharing Cyber Threat Indicators and Defensive Measures

Despite fulfilling requirements of the Cybersecurity Act, we determined the Department faces a number of challenges to effectively sharing cyber threat indicators and defensive measures with other Federal entities and the private sector. Specifically,

- DHS focuses on distributing indicators in a timely manner instead of including additional contextual information that AIS participants desire.
- A cross-domain solution and automated tools are lacking to analyze and share cyber threat information timely.
- Enhanced outreach is needed to increase participation and better coordinate information sharing across Federal agencies and the private sector.

The persistent challenges we identified in information sharing indicate that DHS' adherence to existing legislation alone has been inadequate to ensure that contextual cyber threat indicators or defense measures are shared between Federal entities and the private sector in ways to aid effective responses to evolving threats. Proactive measures on the part of the Federal and non-Federal partners may be needed to ensure the sharing of quality cyber threat information with sufficient details to detect malicious actors, mitigate anomalies, and mount viable defense.

Emphasis Needed on Sharing Quality Cyber Threat Indicators and Defensive Measures

Given that NPPD emphasizes timeliness, velocity, and volume of cyber information sharing, the system DHS currently uses does not provide the

quality, contextual data needed to effectively defend against ever-evolving threats.

As previously discussed, DHS instituted the AIS capability to exchange unclassified cyber threat information among machines as timely and widely as possible across Federal and private sector entities. However, in its current state, AIS does not provide adequate information to effectively protect Federal and private networks. Because the AIS feed is produced through an automated process, with pre-determined data fields, the information may not provide sufficient details to be actionable. For example, AIS may not include specific incidents, tactics, techniques, and procedures that unauthorized users employed to exploit software vulnerabilities. AIS also may not outline effective courses of action for mitigating such threats. Instead of basic cyber threat information, AIS could better assist by providing specific details so that recipients can understand more about the threats and how to counter them. According to an NPPD official, DHS plans to implement the next version of AIS, which could provide more quality information, by the fourth quarter of 2018.

Given AIS' limitations, Federal and private sector entities rely on other systems or participate in other DHS information sharing programs to obtain quality cyber threat data. For example, as previously discussed, the CISCP allows DHS and participating companies to share information about cyber threats, incidents, and vulnerabilities. By design, AIS and CISCP feeds have different methods to populate information and therefore exhibit considerable disparity in data quality. In contrast to the AIS capability that electronically imports pre-determined data points, CISCP analysts directly review and analyze submissions from participating companies to obtain additional details or clarification on the information received. This enables the analysts to provide recipients with more contextual information for determining the appropriate course of action to mitigate potential threats against their networks. While AIS provides quantitative data (i.e., a greater volume of indicators), CISCP provides more qualitative data.

DHS could also benefit from providing more contextual cyber threat indicators and defensive measures to assist Federal and private sector entities with their cyber defense. Without sharing sufficient information, cyber information sharing partners remain restricted in their ability to effectively mitigate evolving security threats and vulnerabilities.

Cross-Domain Solution and Automated Tools Could Promote Timely Sharing and Analysis of Cyber Threat Information

The NCCIC does not have an effective cross-domain solution for sharing unclassified and classified cyber threat indicators and defensive measures with

Federal entities and the private sector. Currently, the NCCIC relies on separate unclassified and classified databases and repositories to gather information on cyber threat indicators. Due to the different classification domains, these databases are hosted separately and are not linked to each other for information sharing purposes. NCCIC cyber analysts we interviewed indicated that they lacked automated capability to process information from the classified repository to the unclassified database. This separation restricted the analysts' ability to compile a complete situational awareness of a potential threat.

The NCCIC also lacks automated tools needed to analyze and share information timely. Such are tools needed for analysts to query multiple sources to enrich the cyber threat data shared. According to NCCIC personnel, the AIS mechanism now requires human intervention—that is, analysts must manually access various, individual databases or repositories to assess the validity of cyber threat indicators and synthesize pertinent information. Given the vast amount of data to sort through, analysts may encounter significant delays in producing information for a single cyber threat indicator. To illustrate, one analyst asserted it could take him up to an hour to review one indicator that could potentially result in a successful cyber attack against Federal or private networks.

Recognizing the need to improve the quality of cyber threat indicators and defensive measures, NPPD approved its *Indicator Management Process Improvement Project Charter* in September 2016. This document was intended to establish a written, measurable process for delivering consistent and high quality indicators to both internal and external sharing partners in a timely manner. Additionally, NPPD approved the *Project Management Plan for CS&C Indicator Management Process Improvement Project* in March 2017 to assess the quality and efficiency of the current indicator management process and develop recommendations for its maturation over time.

The plan includes milestones and deliverables for the project. At the end of our fieldwork, NPPD was taking steps to outline details and map the end-to-end process. However, according to a CS&C official, some milestones had slipped due to the unforeseen need for additional collaboration with related efforts within its divisions. As such, CS&C was behind schedule in delivering the high-level process requirements to stakeholders for their feedback by September 2017. Our review of the plan in May 2017 revealed that NPPD also had yet to establish target dates for completing follow-on tasks such as testing a technology solution for ensuring automated analysis across NCCIC databases, providing training on this capability, and publishing performance measures to ensure it is effective.

By acquiring a cross-domain solution, DHS can provide more detailed cyber information, improve the quality and usefulness of cyber threat reports, and correlate cyber threat indicators and defensive measures across its unclassified and classified environments. Additional automated analytical tools, data standards, and quality controls across NCCIC cyber threat databases would also help streamline vetting processes and ensure uniformity in data format. DHS has taken steps to improve by initiating its Indicator Management Process; however, additional actions are needed to fully implement it and ensure AIS program effectiveness. Through such actions, DHS will be better able to provide Federal entities and the private sector with the quality data they need to mitigate potential risks and threats.

Enhanced Outreach Could Increase Participation and Usefulness of the AIS Program

DHS can enhance its outreach to increase participation and usefulness of the AIS program. At the time of our audit, the NCCIC and DHS' Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division were conducting outreach such as briefings and industry-sponsored events.[7] Typically, SECIR also reached out to private sector entities via teleconference to gather feedback within 90 days of initial AIS deployment to them. However, these calls were one-time only and additional technical assistance to AIS participants was provided upon request.

NCCIC officials acknowledged the need to increase AIS' participation and indicated that they expected to advertise AIS in tandem with other cybersecurity efforts to demonstrate the value of participating in the program. According to one official, SECIR and NCCIC had begun working with private sector organizations that had expressed interest in sharing cyber threat information with the Department via AIS, but needed help overcoming technical, resource, or cultural obstacles to doing so. The NCCIC planned to start a similar outreach effort to gather feedback from Federal entities on AIS effectiveness.

Nevertheless, such outreach efforts were not enough. During interviews, representatives of selected Federal and private sector entities raised the following concerns about NPPD's need to increase training and support for AIS participants. For example:

- Representatives recounted technical problems they had experienced, including connectivity issues and server and file format incompatibility during initial AIS deployment. They had worked through and

[7] SECIR, a division of NPPD/CS&C, is primarily responsible for providing AIS enrollment and outreach services.

successfully resolved such problems with DHS. Still, many suggested that the Department should develop and provide a detailed guide to educate future participants about the AIS deployment process. They also believed DHS needed to offer frequent assistance to new participants to address technical problems.

- Representatives had mixed reviews about the quality and usefulness of the cyber threat indicators shared. For example, one agency representative told us that although DHS provided 11,447 cyber threat indicators in 2016, only 2 or 3 of these indicators were found to be malicious and related to cyber incidents. AIS participants added that many of the indicators received were false positives or redundant information. Although some conceded the accuracy and quality of the indicators were not high, they found the information beneficial. A few representatives suggested that it would be helpful for DHS to alert them to evolving cyber threat patterns by providing regular monthly trend analyses. They also wanted more information regarding the attributes of the cyber threat indicators, such as whether they were unique or repeated indicators, or associated with a specific Nation-state threat.

- Some Federal agency representatives indicated that DHS had not provided sufficient training on how to use the cyber threat indicators and defense measures received through the AIS program. Some private sector representatives indicated they each received a follow-up phone call within 90 days of initial AIS deployment to them, but they got no subsequent calls afterwards to ensure they understood the cyber threat indicators they received. Assistance would have been helpful, as they often were not sure whether indicators were intended for action or for information purposes only.

- Private sector representatives also wanted to be educated on how to digest and use the cyber threat indicators received via AIS, as well as how to send information back to DHS using the system. In general, they wanted a better way to communicate with and provide feedback to DHS.

By enhancing its AIS outreach program to address these and other concerns, the Department can increase participation and better educate Federal and non-Federal entities on AIS services and the utility of the cyber threat indicators shared. DHS can also encourage bi-directional cyber threat indicator sharing across Federal and non-Federal entities. To the extent that Federal and private sector entities can share and exchange cyber threat indicators generated in their respective environments, analysis and correlation of information can be improved, and the Nation's networks can be better protected from a wider range of potential cyber threats.

Security Controls for Systems Used to Share Cyber Threat Indicators and Defensive Measures Could Be Improved

In addition to assessing DHS' implementation of the Cybersecurity Act and identifying related challenges, we found that NPPD can improve security controls for the unclassified and classified systems it uses to process and share cyber threat information. Specifically, we found the component had not implemented all required configuration settings and timely applied security patches on selected MOE and TS MOE workstations and servers we tested. Improperly configured systems and unmitigated security vulnerabilities pose risks to the confidentiality, integrity, and availability of MOE and TS MOE systems, as well as the sensitive information that these two systems store and process.

Improper Configuration Settings

DHS requires that components configure their workstations in accordance with United States Government Configuration Baseline (USGCB) settings. Our assessment revealed that NPPD had implemented 95 percent of the required USGCB settings on the workstations we tested.[8] However, we identified five failed settings on selected workstations related to the following areas:

- File access permissions could allow users to gain unauthorized access to folders and files.
- Remote desktop access could allow unauthorized users to gain elevated permissions to the network.
- Network logon time was not configured to synchronize with an authorized server, although essential for user authentication, audit trails, and accountability.
- Windows registry was not properly configured to prevent computer names from being identified, potentially providing attackers with useful information for gaining access to hidden systems on the network.

Subsequent to our fieldwork, NPPD provided supporting evidence that the component had implemented the settings related to file permissions, remote desktop access, and network log on time. Still, NPPD has not provided

[8] USGCB settings are the core set of security related configuration settings that all Federal agencies must implement on its workstations. The baseline includes controls such as user access, password management, auditing, and computer services.

documentation to support that the component has implemented the Windows registry setting for workstation identification.

Inadequate Patch Management

Per DHS Sensitive Systems Policy 4300A, components must also manage systems to reduce vulnerabilities through testing, promptly installing patches, and eliminating or disabling unnecessary services. However, we detected 20 unique vulnerabilities during our security vulnerability assessments of MOE and TS MOE. Critical and high-risk vulnerabilities that are successfully exploited may result in significant data loss and system disruption. Following are specific examples of the critical and high-risk vulnerabilities we detected.

- A Java security update had not been applied on affected workstations that could be exploited to cause a denial of service attack.
- An eXtensible Markup Language vulnerability had not been addressed and could allow unauthenticated users to remotely execute code on affected workstations.[9]
- Three unpatched vulnerabilities could be exploited to provide users elevated permissions to access affected servers.

Table 2 outlines the number of critical and high-risk vulnerabilities we detected during our testing.

Table 2: Unique Vulnerabilities Identified on MOE and TS MOE

Systems Tested		Unique Vulnerabilities Identified	
		Critical	High
MOE	489 workstations	0	7
	13 servers	0	6
TS MOE	19 workstations	0	3
	4 servers	1	3
TOTALS:		**1**	**19**

Source: DHS OIG

We alerted NPPD officials regarding the specific vulnerabilities we identified through our testing. The NPPD officials provided no explanation as to why the patches were missing. However, they outlined plans to mitigate the vulnerabilities by applying proper security patches or changing NPPD's security

[9] XML is a set of rules for encoding documents in a format that is both human-readable and machine-readable.

plan or policy. As of May 2017, NPPD had taken actions to apply some of the missing patches and had created corrective action plans to address the others.

Given the extreme importance of its cybersecurity and critical infrastructure protection mission and responsibilities, NPPD must ensure that its workstations are secure from unauthorized access. Implementing required workstation configuration settings will reduce the risk of sensitive information being exposed and exploited. Timely application of security patches is critical to mitigating potential system vulnerabilities. Without remediating identified vulnerabilities by implementing required configuration settings and system updates, sensitive cyber mission data may be open to compromise.

Recommendations

We recommend that the Assistant Secretary for Cybersecurity and Communication, National Protection and Programs Directorate:

Recommendation 1. Revise milestones and deliverables, including all necessary tasks and activities for ensuring accomplishment of the indicator management process improvement project within specific timeframes.

NPPD Comments to Recommendation 1

NPPD concurred with recommendation 1. CS&C has already revised the project plan as recommended and provided a copy to OIG. CS&C requested that OIG consider this recommendation resolved and closed.

OIG Analysis of NPPD Comments

We agree that the steps NPPD has taken satisfy the intent of this recommendation. We considered this recommendation closed.

Recommendation 2. Establish an acquisition strategy for obtaining the tools and technologies needed to provide a cross-domain solution for sharing and processing cyber threat information between the classified and unclassified repositories.

NPPD Comments to Recommendation 2

NPPD concurred with recommendation 2. NPPD acknowledged that the component must identify and deploy a cross-domain capability for sharing and processing cyber threat information between the classified and unclassified indicator repositories. A cross-domain capability is part of DHS' roadmap for National Cybersecurity Protection Systems Information Sharing. In fiscal year

2018, the Network Security Deployment Division plans to evaluate potential cross-domain solutions for compliance with Unified Cross-Domain Management Office standards and requirements of NCCIC. Once appropriate trade studies and analyses are conducted, the National Cybersecurity Protection Systems program management office will analyze the results and establish a plan for obtaining and implementing a cross-domain solution. The estimated completion date is September 30, 2018.

OIG Analysis of NPPD Comments

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

Recommendation 3. Actively promote participation in the Automated Indicator Sharing program through enhanced outreach that includes providing additional products, services, technical assistance, information sharing forums, and training courses for Federal and private sector entities.

NPPD Comments to Recommendation 3

NPPD concurred with recommendation 3. NCCIC is working with other CS&C divisions, specifically the SECIR and Federal Network Resilience divisions, to promote AIS by helping organizations that may experience technical, resource, or cultural hurdles that can impede their participation. NCCIC has established a goal to ensure participation from all 16 critical infrastructure sectors, including engagement with the respective sector-specific agencies. The estimated completion date is June 30, 2018.

OIG Analysis of NPPD Comments

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

Recommendation 4. Implement the required United States Government Configuration Baseline configuration settings on the unclassified and classified Mission Operating Environments, or follow applicable DHS policy to submit a waiver to acknowledge and accept the risk of non-compliance.

NPPD Comments to Recommendation 4

NPPD concurred with recommendation 4. The National Cybersecurity Protection Systems program management office maintains a waiver signed by the DHS Chief Information Security Officer authorizing the Network Security Deployment Division to use the *Defense Information System Agency Security Technical Implementation Guidelines* as the system baseline. Additionally, the NPPD Chief Information Security Officer recently released a memorandum directing NPPD sub-components to scan systems using the *Defense Information System Agency Security Technical Implementation Guidelines* audit policies. Copies of both the waiver and the NPPD memorandum have been provided to OIG under separate cover. CS&C requested that OIG consider this recommendation resolved and closed.

OIG Analysis of NPPD Comments

The screenshot that NPPD provided was for a server, not for workstations. This recommendation is unresolved and will remain open until vulnerabilities identified on the workstations are mitigated and supporting documentation is provided.

Recommendation 5. Mitigate identified vulnerabilities by applying required patches, or accept the risk by documenting the weaknesses in the system security plans for the unclassified and classified Mission Operating Environments.

NPPD Comments to Recommendation 5

NPPD concurred with recommendation 5. NPPD indicated that the finding related to eXtensible Markup Language was addressed prior to the conclusion of our audit. Since the conclusion of the audit, the Network Security Deployment Division has modified configuration management practices (specifically, applied baseline configuration and configuration change control). Further, the security operation center is configured to provide daily alert for "new" vulnerabilities. CS&C requested that OIG consider this recommendation resolved and closed.

OIG Analysis of NPPD Comments

Additional documentation is needed to support that security patches are applied consistently on all workstations. This recommendation is unresolved and will remain open until vulnerabilities identified on workstations are mitigated and supporting documentation is provided.

Appendix A
Objective, Scope, and Methodology

The DHS OIG 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. We conducted an evaluation of the Department's progress in meeting cybersecurity information sharing requirements, pursuant to Section 107 of the *Cybersecurity Act of 2015*.

To achieve our objective, we interviewed selected personnel from DHS components with cybersecurity missions (i.e., NPPD, Office of Policy, ICE, and Secret Service). We reviewed DHS policies and procedures for sharing cyber threat indicators and defensive measures with other Federal Government and private sector organizations. We analyzed the mechanisms and methodologies used for sharing the cyber threat information, including the removal of unrelated personal information as required by the Act. We assessed whether DHS properly classified cyber threat indicators and defensive measures shared its information sharing partners. We also determined whether DHS could account for security clearances granted to private sector users of the cyber threat information shared. We evaluated the effectiveness of security controls on the MOE and TS MOE systems that DHS and its components use to collect, process, and generate cyber threat indicators and defense measures. Further, we attended congressional hearings regarding the status of DHS AIS partnerships with the Federal entities and the private sector.

We judgmentally selected our sample of AIS participants to interview for this evaluation. We met with representatives of the Departments of State, Health and Human Services, and Veterans Affairs; the National Aeronautics and Space Administration; and selected critical infrastructure sectors to obtain their perspectives on the effectiveness of the AIS program. We also met with non-Federal AIS participants. Under AIS' publicly-available sharing guidance, a non-Federal entity sharing information with DHS must provide consent before the Department can share its identity with other Federal entities. Based on the consent provided, we identified 15 non-Federal entities and ultimately interviewed officials from 6 private companies/organizations. To limit the scope of our review, we did not interview representatives of state, local, territorial governments, or foreign partners.

We conducted this review between January and June 2017 under the authority of the *Inspector General Act of 1978*, as amended, and according to the Quality Standards for Inspections and Evaluations issued by the Council of the Inspectors General on Integrity and Efficiency. We believe that the evidence

obtained provides a reasonable basis for our findings and conclusions based upon our review objectives. Major OIG contributors to the review are identified in appendix D.

Appendix B
NPPD Comments to the Draft Report

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

Homeland Security

September 12, 2017

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

FROM: Jeanette Manfra
Assistant Secretary
Office of Cybersecurity & Communications
National Protection and Programs Directorate

SUBJECT: Management's Response to OIG Draft Report: "Review of DHS' Implementation of the Cybersecurity Act of 2015" (Project No. OIG-17-015)

Thank you for the opportunity to review and comment on this draft report. The National Protection and Programs Directorate (NPPD), specifically the Office of Cybersecurity and Communications (CS&C), appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

NPPD/CS&C is pleased to note OIG's positive recognition that the Department has adequately addressed the information sharing requirements of Title I, Section 107 of the *Cybersecurity Act of 2015*. Specifically, OIG notes that we have developed adequate policies and procedures and the capability to share cyber threat indicators and defensive measures. OIG also recognized that we properly classified the indicators and defensive measures and accounted for the security clearances of private sector recipients of the shared information.

NPPD/CS&C also appreciates OIG's efforts in conducting interviews with select consumers of the cyber threat indicators and defensive measures that we share. The results of the interviews found that this shared information was used to improve their network security controls and to detect malicious actors, mitigate anomalies, and possible threats to their networks.

The draft report contained five recommendations with which NPPD/CS&C concurs. Please see the attached for our detailed response to each recommendation.

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.

Attachment

Attachment: DHS Management Response to Recommendations Contained in OIG-17-015

OIG recommended that the Assistant Secretary for Cybersecurity and Communication, National Protection and Programs Directorate:

Recommendation 1: Revise milestones and deliverables, including all necessary tasks and activities for ensuring accomplishment of the indicator management process improvement project within specific timeframes.

Response: Concur. CS&C has already revised the project plan as recommended and provided a copy to OIG under separate cover. We request that OIG consider this recommendation resolved and closed.

Recommendation 2: Establish an acquisition strategy for obtaining the tools and technologies needed to provide a cross-domain solution for sharing and processing cyber threat information between the classified and unclassified repositories.

Response: Concur. NPPD/CS&C, specifically the Network Security Deployment (NSD) division, acknowledges that NPPD must identify and deploy a cross-domain solution for sharing and processing cyber threat information between the classified and unclassified indicator repositories. A cross domain solution capability is part of the roadmap for the National Cybersecurity Protection System (NCPS) Information Sharing (Block 2.2). In fiscal year (FY) 2018, NSD plans to conduct analysis on the cross domain solutions that are compliant with Unified Cross Domain Management Office standards and meet the requirements of the National Cybersecurity & Communications Integration Center (NCCIC). Once appropriate trade studies and analysis are conducted, the NCPS program management office will analyze the results and establish a plan for obtaining and implementing a cross domain solution.
Estimated Completion Date (ECD): September 30, 2018.

Recommendation 3: Actively promote participation in the Automated Indicator Sharing (AIS) program through enhanced outreach that includes providing additional products, services, technical assistance, information sharing forums, and training courses for Federal and private sector entities.

Response: Concur. NCCIC is working with CS&C divisions, specifically the Stakeholder Engagement and Critical Infrastructure Resiliency and Federal Network Resilience divisions, to promote AIS by helping organizations that may have technical, resource or cultural hurdles that impede them from participating. The NCCIC has a goal to ensure participation across all sixteen critical infrastructure sectors, including engagement with the respective Federal sector specific agencies. ECD: June 30, 2018.

Recommendation 4: Implement the required United States Government Configuration Baseline (USGCB) configuration settings on the unclassified and classified Mission Operating

Environments, or follow applicable DHS policy to submit a waiver to acknowledge and accept the risk of non-compliance.

Response: Concur. The NCPS maintains a waiver signed by the DHS Chief Information Officer (CIO) authorizing NSD to use the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) as the system baseline. The OIG audit team acknowledged the DISA STIG's are more stringent than the USGCB. Additionally, the NPPD Chief Information Security Officer recently released a memorandum directing the NPPD sub-components to scan systems using the DISA STIG audit policies. Copies of both the waiver and the NPPD memorandum have been provided to OIG under separate cover. We request that OIG consider this recommendation resolved and closed.

Recommendation 5: Mitigate identified website vulnerabilities by applying required patches, or accept the risk by documenting the weaknesses in the system security plans for the unclassified and classified Mission Operating Environments.

Response: Concur. The finding related to eXtensible Markup Language (XML) was addressed prior to the conclusion of the audit (NSD provided documentation of this to the OIG in May 2017). Since the conclusion of the audit, NSD has modified the Configuration Management practices (specifically the application of CM-2 Baseline Configuration and CM-3 Configuration Change Control). Furthermore, security center has been configured to alert on the Nessus daily results for *new* software vulnerabilities. We request that OIG consider this recommendation resolved and closed.

Appendix C
Responses to the Office of the Inspector General of the Intelligence Community

Policies, Procedures, and Guidelines
1. Does your agency have policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government? Please list.
Comment: DHS has developed or assisted in the development of the following policies and procedures: • Federal Government Sharing Guidance • Non-Federal Entity Sharing Guidance (sec 105 (a)) • Operational Procedures (105) (a) • Privacy and Civil Liberties Guidelines (sec 105 (b)) • Automated Indicator Sharing (AIS) Brokering • Indicator Management Standard Operating Procedures • Cyber Threat Management • Intelligence Triage Process • Indicator Vetting Process • US-CERT Cyber Information Handling Guidelines
1.a. Do these policies, procedures, and guidelines include guidance for removing information not directly related to a cybersecurity threat that is personal information of a specific individual or information that identifies a specific individual? Please provide title of policy, procedure, or guidance.
Comment: Yes. The following policies and procedures include guidance for removing personal information or other information that is not related to a cybersecurity threat: • Sharing of Cyber Threat Indicators and Defensive Measures by Federal Government under the Cybersecurity Information Sharing Act of 2015, February 2016. • Privacy and Civil Liberties Guidelines: Cybersecurity Information Sharing Act of 2015, June 2016. • AIS Brokering Between the Non-Federal Entities Sharing Community and the Federal Entities Sharing Community, July 2016. • US-CERT Cybersecurity Information Handling Guidelines, October 2016.

1.b. Are the policies, procedures, and guidelines for sharing cyber threat indicators within the Federal Government sufficient?
Comment: Yes. The policies, procedures, and guidelines are currently adequate for sharing cyber threat indicators in accordance with the Cybersecurity Act. However, Federal agencies would benefit from being able to share more detailed and actionable information.
1.c. How did your agency determine sufficiency?
Comment: We reviewed the policies, procedures, and guidelines listed in response 1 and interviewed selected NPPD personnel. DHS has fulfilled the requirements as mandated by Section 103 of the *Cybersecurity Act of 2015*, which directed the Director of National Intelligence, the Secretaries of Defense and Homeland Security, and the Attorney General, in consultation with the heads of the appropriate Federal entities to jointly develop and issue procedures to facilitate and promote timely sharing of cyber threat indicators and defensives measures with Federal and Non-Federal entities.
Sharing Cyber Threat Indicators and Defensive Measures with the Private Sector
2.a. Has your agency shared cyber threat indicators and defensive measures with the private sector?
Comment: Yes. DHS has shared 210,087 sharing unclassified cyber threat indicators with its private sector partners via AIS since March 2016. During the period of October 2015 to April 2017, the Department has shared 2,290 classified cyber threat indicators with the private sector.
2.b. Did your agency properly classify the cyber threat indicators and defensive measures shared with the private sector?
Comment: Yes. DHS has classified cyber threat indicators using derivative classification. Further, the original classification of the cyber threat indicators remained with the Original Classification Authority. DHS uses additional security classification guides (e.g., the National Cybersecurity Protection System (also known as EINSTEIN) and Enhanced Cybersecurity Services) to classify cyber threat indicators.

2.c. How did your agency determine whether the shared cyber threat indicators and defensive measures were properly classified?
Comment: Based on the Original Classification Authority, cyber threat indicators maintain the same classification unless a tear line report is provided to declassify the information.[10] DHS uses derivative classification on the cyber threat indicators received. According to DHS analysts, 95 percent of cyber threat indicators received from external sources are derivatively classified and the remaining 5 percent are originally classified through internal reporting.
Accounting for Security Clearances
3. How does your agency account for the number of security clearances authorized for sharing cyber threat indicators and defensive measures with the private sector?
Comment: As of May 2017, the Department has granted 1,631 active security clearances and 312 pending applications under various DHS' information sharing programs. However, DHS does not track the number of clearances issued for the purpose of sharing information under its AIS program alone. Since AIS shares unclassified cyber threat indicators, security clearances are not required.
Using and Disseminating Cyber Threat Indicators and Defensive Measures Shared by Other Federal Agencies
4.a. Has your agency used and disseminated cyber threat indicators and defensive measures shared by other Federal agencies?
Comment: Yes. DHS has used cyber threat indicators shared by other Federal agencies, such as the Departments of Energy, State, and Veterans Affairs; Secret Service, the National Security Agency, and the Intelligence Community.
4.b. Did your agency use and disseminate the shared cyber threat indicators and defensive measures appropriately?
Comment: Yes. Based on the classification of cyber threat indicators, DHS shares unclassified indicators via AIS according to the Department's Traffic Light Protocol (TLP) and classified indicators under the business rules of the EINSTEIN 3 Accelerated and Enhanced Cybersecurity Services programs.

[10] Tear line reports are portions of an intelligence report or product that provide the substance of a more highly classified or controlled report without identifying sensitive sources, methods, or other operational information. Tear line reports release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification.

4.c. How did your agency determine if the use and dissemination of shared cyber threat indicators and defensive measures was appropriate?
Comment: DHS uses the TLP to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audiences. It employs four colors (red, amber, green, and white) to indicate expected sharing boundaries to be applied by the recipients properly. For classified cyber threat indicators, cyber analysts work with NSA personnel to sanitize cyber threat indicators and defensive measures to remove personal information before sharing.
Sharing Cyber Threat Indicators and Defensive Measures with Other Federal Agencies
5.a. Has your agency shared cyber threat indicators and defensive measures with other Federal agencies?
Comment: Yes. Since June 2017, DHS has shared 210,087 cyber threat indicators via AIS with 33 Federal entities. In total, the Department has shared 513,639 cyber threat indicators through additional data feeds, CISCP and FedGov, since June 2017.
5.b. Did your agency share the cyber threat indicators and defensive measures in a timely and adequate manner with appropriate entities or, if appropriate, made publicly available?
Comment: Yes. Based on our interviews with representatives of other Federal departments, cyber threat indicators and defensive measures were shared in a timely and adequate manner. Additionally, DHS shares unclassified cyber threat indicators via AIS as they are received. If a manual review is required, DHS will share all other information, and mark the appropriate data fields as "under review," and release the relevant information as quickly and as operationally practical.
5.c. Have other Federal entities shared cyber threat indicators and defensive measures with your agency in a timely, adequate, and appropriate manner?
Comment: Yes. Based on our interviews with selected officials, the National Cybersecurity and Communications Integration Center, Department of Energy, and National Security Agency share cyber threat indicators with DHS timely and on a regular basis. In addition, representatives from the Departments of State and Veterans Affairs, as well as Secret Service, within DHS, indicated that their agencies share cyber threat indicators with DHS upon receipt.
5.d. How did your agency determine timeliness, adequacy and appropriateness of sharing the information?
Comment: DHS determines "timeliness" based on the "real-time" sharing of cyber threat indicators and other relevant information after analyst review, and as quickly as operationally practical.

DHS' Sharing Capability and Processes
6.a. How many cyber threat indicators and defensive measures have non-Federal entities shared with the Department of Homeland Security through the capability and process developed under section 105(c)?
Comment: Non-Federal entities have shared 181,307 cyber threat indicators and 2 defensives measures with DHS since November 2016.
6.b. How many of those cyber threat indicators and defensive measures reported for 6.a. above did the Department of Homeland Security share with other Federal entities?
Comment: DHS subsequently shared all 181,307 cyber threat indicators and 2 defensive measures with other Federal entities. All cyber threat indicators and defensive measures received via AIS are shared with other Federal entities.
Cyber Threat Indicators and Defensive Measures Received from Other Federal Agencies
7. How many cyber threat indicators and defensive measures from non-Federal entities did the Department of Homeland Security relay to your agency?
Comment: DHS shared all 181,307 cyber threat indicators and 2 defensive measures with other Federal entities. All cyber threat indicators and defensive measures received via AIS are shared with other Federal entities.
Personal Information Violations
8.a. Did any Federal or non-Federal entity share information with your agency that was not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual in violation with this title?
Comment: According to DHS officials, there has been no unauthorized release of personally identifiable information since the start of the AIS program in March 2016. DHS performs a manual review to redact any personal information and ensure it is not released. .
8.b. Please include a description of the violation.
Comment: Not applicable. See response 8a.
Effects on Federal Agencies Sharing Cyber Threat Indicators and Defensive Measures
9.a. Was there an effect of your agency sharing cyber threat indicators and defensive measures with the Federal Government on privacy and civil liberties of specific individuals?
Comment: None.

9.b. What was the effect on privacy and civil liberties of specific individuals?
Comment: None.
9.c. How did your agency quantitatively and qualitatively assess the effect?
Comment: Not applicable. See responses 9a-b.
9.d. Did your agency receive any notices regarding a failure to remove information that WAS NOT directly related to a cybersecurity threat AND were any of those notices related to personal information of a specific individual or information that identified a specific individual?
Comment: Not applicable. See responses 9a-b.
9.e. How many notices did your agency receive?
Comment: Not applicable. See responses 9a-b.
9.f. Did your agency issue any notices regarding a failure to remove information that WAS NOT directly related to a cybersecurity threat AND were any of those notices related to personal information of a specific individual or information that identified a specific individual?
Comment: No. See response 8a.
9.g. How many notices did your agency issue?
Comment: None. See response 8a.
Steps Taken to Reduce Adverse Effects
10.a. Were the steps taken by your agency to reduce adverse effects from the activities carried out under this title on the privacy and civil liberties of U.S. persons adequate?
Comment: Yes. DHS and Department of Justice jointly developed the Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, June 2016 and United States Computer Emergency Readiness Team Cybersecurity Information Handling Guidelines, October 2016 to address privacy and civil liberties issues. DHS also implemented privacy controls to prevent PII violations.
10.b. How did your agency determine adequacy of the steps taken?
Comment: DHS manually reviews disclosures and removes PII to ensure there is no unauthorized release. Additionally, DHS performed a privacy impact assessment on AIS, including a review of privacy, civil liberties, and other compliance concerns and risks.

Potential Barriers to Sharing
11.a. Has your agency identified any barriers that adversely affected the sharing of cyber threat indicators and defensive measures among Federal entities?
Comment: Yes.
11.b. Please describe the barriers and the effect the barriers have on the sharing of cyber threat indicators and defensive measures.
Comment: We have identified the following barriers and challenges to sharing cyber threat indicators: • The system DHS currently uses does not provide the quality, contextual information needed to ensure appropriate responses to evolving threats. • A cross-domain solution and automated tools are lacking to analyze and share cyber threat information timely. • Enhanced outreach is needed to increase participation and better coordinate information sharing across Federal agencies and the private sector.

Appendix D
Major Contributors to This Report

Chiu-Tong Tsang, Director
Tarsha Cary, Audit Manager
Brandon Barbee, Audit Manager
Jasmine Raeford, IT Specialist
Yusuf Lane, IT Auditor
Amber May, IT Specialist
Tunisia Phifer, IT Auditor
Mahfuza Khanam, IT Auditor
Tonya McKinnon, IT Auditor
Thomas Rohrback, Branch Chief
David Bunning, IT Specialist
Shawn Ward, Referencer

Appendix E
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs 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
DHS Chief Information Officer
DHS Chief Information Security Officer
Privacy Office
Chief Information Officer, NPPD
Executive Associate Director of Homeland Security Investigations, ICE
Deputy Under Secretary, Office of Cybersecurity and Communications, NPPD
Deputy Assistant Secretary for Cyber Policy, Office of Policy
Director, 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

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu