UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

September 30, 2019

MEMORANDUM FOR: André Mendes
Acting Chief Information Officer

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *The Department Needs to Improve Its Capability to Effectively Share Cyber Threat Information*
Final Report No. OIG-19-026-A

This final report provides the results of our audit to assess the Department of Commerce's (the Department's) cybersecurity information sharing program, consistent with the Cybersecurity Information Sharing Act of 2015 (CISA).[1] Our audit objective was to determine the capabilities and practices of the Department to carry out cybersecurity information sharing.

We observed that the Department ingests cyber threat information from many different sources. The Department's Enterprise Security Operations Center (ESOC) uses the Commerce Threat Intelligence Portal (CTIP) for the internal dissemination and sharing of information from these sources among the Department's bureaus. Despite recent CTIP software upgrades, we observed several challenges the Department faces in sharing cyber threat information effectively. Specifically,

- the Department lacked an internal automated sharing capability;
- the CTIP application was not accessible by all bureaus; and
- the Department lacked adequate information sharing policies, procedures, and training.

This report includes recommendations to strengthen the effectiveness of the internal cyber threat information-sharing program. See appendix A for specific details on our objective, scope, and methodology.

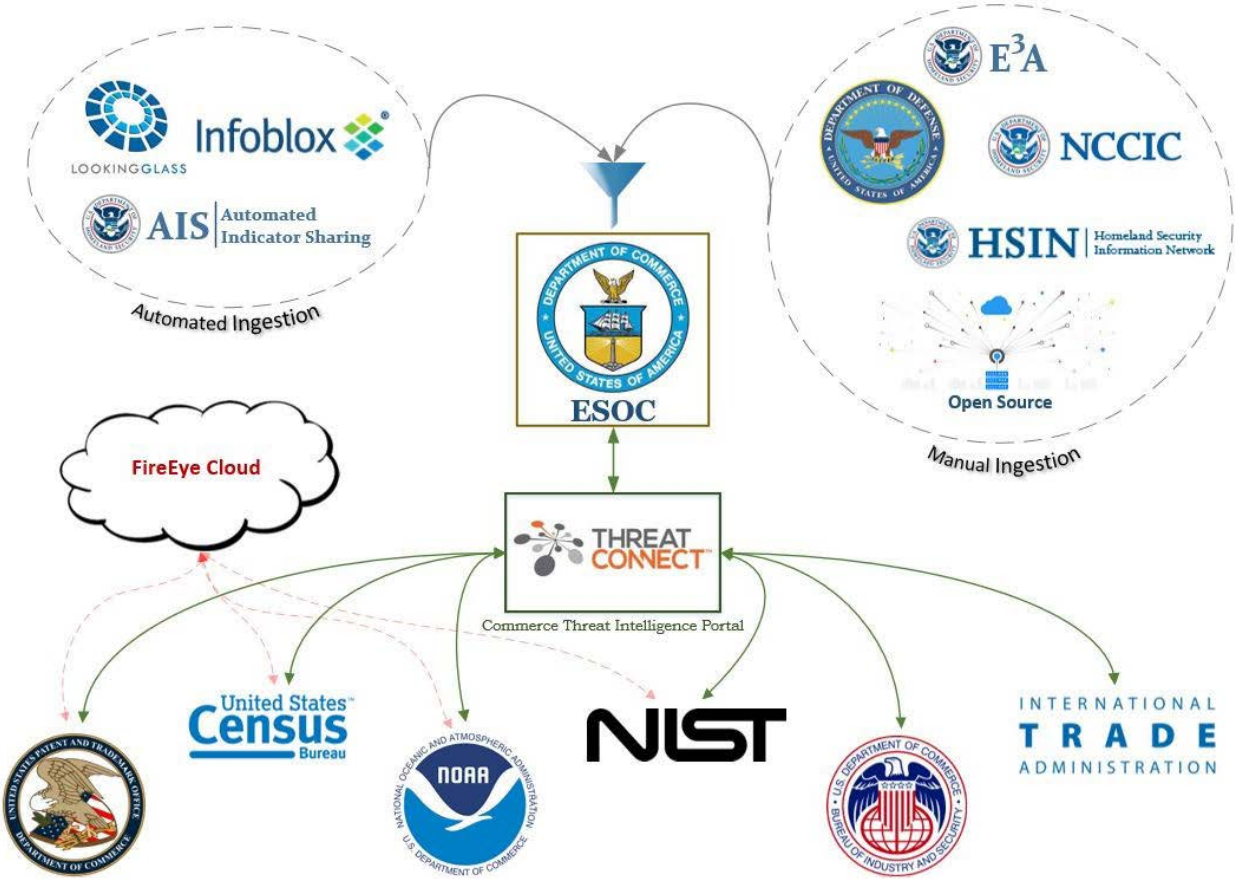
Background

The service level agreement between ESOC and the Department's bureaus describes services to be delivered by ESOC. Among other responsibilities, ESOC is tasked to facilitate the timely sharing of cyber threat information at machine speed, when possible. In support of this function, ESOC operates CTIP for internal cyber threat information dissemination and sharing among the bureaus. Cyber threat information collected from federal, commercial, and open-source

[1] Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242, 2936 (2015); 6 U.S.C. § 1501, *et seq.*

channels is ingested by ESOC and internally distributed through CTIP (see figure 1). ESOC interfaces with the U.S. Department of Homeland Security's (DHS's) Automated Indicator Sharing (AIS) capability on behalf of the entire Department.[2] ESOC also facilitates weekly conference calls that are available to the bureaus to discuss cyber threat trends and major concerns.

Figure 1. Department of Commerce Information Sharing[a]



Source: OIG

[a] We judgmentally selected six Department bureaus to include as part of this audit (that is, U.S. Patent and Trademark Office (USPTO), U.S. Census Bureau (Census), National Oceanic and Atmospheric Administration (NOAA), National Institute of Standards and Technology (NIST), Bureau of Industry and Security (BIS), and International Trade Administration (ITA)). It is for this reason only six of the Department's bureaus are depicted within this figure. See appendix A for more details on our objective, scope, and methodology.

ESOC rarely shares cyber threat information outside of the Department.[3] Information shared outside the Department is primarily in the form of cybersecurity incident reports that are

[2] DHS developed the AIS capability to fulfill the requirement mandated by CISA. *See* 6 U.S.C. § 1504(c). Federal government agencies and bureaus are encouraged, but not required, to use the capability.

[3] ESOC participates in weekly conference calls hosted by DHS's National Cybersecurity and Communications Integration Center (NCCIC) to discuss cyber threat trends and major concerns. Information may be exchanged in this setting as discussions take place.

delivered to the U.S. Computer Emergency Readiness Team (US-CERT), a component of the DHS' Cybersecurity and Infrastructure Security Agency.

Department bureaus primarily use CTIP to ingest information for local Security Operations Center (SOC) activities. The bureaus possess the ability to upload cyber threat information to CTIP, but this is rarely used due to how uncommon it is to uniquely identify a new malicious activity. Most threats are already known and are brought to the attention of the bureaus via ingested threat information. In addition to CTIP, bureaus collect cyber threat information through additional sources, including private vendors and open-source channels. Some bureaus have also implemented FireEye[4] cybersecurity solutions that include automated sharing as an additional feature (i.e., it is not the primary purpose of the tool). For example, FireEye's Email Threat Prevention (ETP) security service[5] integrates dynamic two-way sharing as an opt-in feature, which is leveraged by USPTO, Census, NOAA, and NIST.[6] This feature automatically pushes and pulls identified malicious indicators to and from the FireEye cloud so all opted-in customers have access to the aggregated indicators (see figure 1).

While some of the bureaus (e.g., Census, NIST, NOAA, and USPTO) use CTIP only as a supplemental tool, other bureaus (e.g., BIS and ITA) rely on CTIP as their primary source of cyber threat information.

Findings and Recommendations

As part of our audit, we identified improvements needed in the Department's cybersecurity information sharing program. Despite a CTIP software update in January 2019 that brought significant improvements and the capability to implement new features, we observed that the Department still faces a number of challenges to share cyber threat information effectively.

I. The Department Lacked an Internal Automated Sharing Capability

The current implementation of CTIP lacks an automated sharing capability, resulting in a tedious manual process to ingest or share cyber threat information. The lack of an automated system to handle cyber threat information presents CTIP users with an unmanageable amount of data to manually process. For example, ESOC ingests more than 3 million cyber threat indicators every week. Several bureaus regard the absence of automated ingestion as a major drawback that significantly reduces the value of the tool. In fact, one of the bureaus stopped using CTIP altogether, and instead used other tools and capabilities with automation to ingest cyber threat information. The ever-evolving landscape and sheer quantity of cyber threats demand the automation of cyber threat information ingestion for manageability and effectiveness.

[4] FireEye is a private cybersecurity service provider.

[5] FireEye's ETP security service is FedRAMP-authorized and the Privacy Impact Assessment was reviewed and approved by a Department privacy officer.

[6] The dynamic two-way sharing feature is not enabled by default. Participants must take action to enable the feature.

According to ESOC, the newly updated CTIP has the capability to support automation through an Application Programming Interface, but has not been implemented because licensing and interconnection agreements needed to be updated first.

II. The CTIP Application Was Not Accessible by All Bureaus

Prior to the January 2019 CTIP software upgrade, CTIP required users to access the portal via a virtual private network (VPN) connection. However, the software upgrade made CTIP more accessible by allowing access through a web browser from Department internal networks. It also integrated the use of personal identity verification (PIV) cards for user authentication. These technical changes produced unintended consequences that impeded ITA and USPTO access. For example:

- ITA was unable to connect to CTIP from January through April 2019 because its network was not recognized as one belonging to the Department after the software upgrade. ITA worked with ESOC and NIST to resolve this issue, and subsequently, CTIP access was restored during our audit in April 2019.
- USPTO was unable to connect to the new implementation of CTIP due to an issue with PIV card authentication. Specifically, USPTO users encountered an authentication error when attempting to log in to CTIP, because the authentication mechanism would attempt to use incorrect certificates from the users' PIV cards. The CTIP software did not provide an option to specify which certificate to use for authentication.[7] ESOC asserted that USPTO implements its PIV card structure differently than other bureaus, which is why the authentication mechanism does not currently support USPTO PIV cards. ESOC and USPTO were still working together to resolve this issue as of July 2019. As a temporary workaround, ESOC was delivering cyber threat information to USPTO via secure file transfer.

III. The Department Lacked Adequate Information Sharing Policies, Procedures, and Training

Although many of the requirements in CISA are not binding on the Department, CISA requires the Department to follow the procedures and guidance promulgated under CISA by DHS, Department of Justice (DOJ), Department of Defense (DOD), and the Office of the Director of National Intelligence (ODNI).[8] We found the Department's cyber threat information sharing policies and procedures did not integrate those procedures and guidance. For example, *Sharing of Cyber Threat Indicators and Defensive Measures by the*

---

[7] USPTO personnel PIV cards contain more than one certificate.

[8] *See* 6 U.S.C. §§ 1502, 1504. These procedures include: (1) ODNI, DHS, DOD, & DOJ, February 16, 2016. *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015*; (2) DHS & DOJ, June 15, 2016. *Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government;* and (3) DHS & DOJ, June 15, 2018. *Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015.*

Additional guidance is provided for non-federal entities:
DHS & DOJ, June 15, 2016. *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*.

Federal Government under the Cybersecurity Information Sharing Act of 2015, section 9.3, describes a notification provision for notifying entities "…that have received a cyber threat indicator or defensive measure from a federal entity under this title that is known or determined to be in error or in contravention," which was not included in Departmental procedures.

The required procedures and guidance were not integrated with the Department's cyber threat information sharing policies and procedures because ESOC personnel were not aware of the documents. We made them aware of these documents during our audit, and as of July 2019, they were reviewing and incorporating these documents into Department cyber threat information sharing policies and procedures.

Additionally, several CTIP users expressed concern regarding a lack of training and procedural documents on how to use CTIP. Only one of the Department's bureaus was aware of documentation (e.g., user guides and standard operating procedures) that could assist in its use of CTIP. All other bureaus possessed only one document with instructions on gaining access to the CTIP application. All documentation, however, was outdated and no longer applicable due to the Department's software upgrade to CTIP.

As of July 2019, ESOC was drafting a comprehensive user guide on how to use the newly upgraded CTIP, but it was yet to be completed and made available to the Department's bureaus.

Recommendations

We recommend that the Chief Information Officer do the following:

1. Finalize CTIP licensing and interconnection agreements and utilize the CTIP Application Programming Interface to automate Department bureaus' ingestion of cyber threat information.
2. Ensure that all Department bureaus have access to CTIP.
3. Ensure information sharing policies and procedures are compliant with the applicable documents that were created by DHS, DOJ, DOD, and ODNI.
4. Complete a comprehensive CTIP user guide and make it available to all Department bureaus.

Summary of Agency Response and OIG Comments

On September 25, 2019, we received the Department's response to the draft report's findings and recommendations, which we include within this final report as appendix B. The Department concurred with our findings and recommendations. This final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days.

We appreciate the cooperation and courtesies extended to us by the Department's and bureaus' staff during this audit. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Dr. Ping Sun, Director for IT Security, at (202) 482-6121.

cc: Joselyn Bingham, Audit Liaison, OCIO
Maria Dumas, IT Security Audit Action Officer, OCIO
Bharat Dass, Alternate IT Security Audit Action Officer, OCIO
Jason Schwartz, IT Security Audit Support, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary
Carol Rose, Chief Financial Officer and Administrative Director, BIS
Jennifer Kuo, GAO/OIG Audit Liaison, BIS
Dawn Taylor, GAO/OIG Program Manager, BIS
Kevin B. Smith, CIO, Census Bureau
Colleen Holzbach, Program Manager for Oversight Engagement, Census Bureau
Jean McKenzie, IT Security Audit Liaison, Census Bureau
Rona Bunn, Acting CIO, ITA
Jennifer Eveland, Senior Management and Program Analyst, ITA
Joe Ramsey, Audit Liaison, ITA
Blanche Ziv, Director of the Operational Excellence Division, ITA
Susannah Schiller, Acting CIO, NIST
Amy Egan, Audit Liaison, NIST
Catherine Fletcher, Audit Liaison, NIST
Zack Goldstein, CIO, NOAA
Rhonda Lawrence, Audit Liaison, NOAA
Jamie Holcombe, CIO, USPTO
Welton Lloyd, Audit Liaison, USPTO
Sarah Harris, General Counsel, USPTO
Sean Mildrew, Acting Chief Financial Officer, USPTO

Appendix A.
Objective, Scope, and Methodology

The objective of this audit was to determine the capabilities and practices of the Department to carry out cybersecurity information sharing. To accomplish this objective, we reviewed policies, procedures, and guidelines associated with Department information sharing activities. We also distributed questionnaires and met with ESOC and six judgmentally selected bureau SOC officials. Those six bureaus, each of which operates an independent SOC, were the following:

- BIS
- Census
- ITA
- NIST
- NOAA
- USPTO

We conducted our review from December 2018 through April 2019 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, dated April 26, 2013. We conducted our fieldwork at Department headquarters and bureau sites in Suitland, Maryland; Silver Spring, Maryland; Gaithersburg, Maryland; and Alexandria, Virginia.

We conducted this audit in accordance with 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 the findings and conclusions based on the audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix B.
Agency Response

UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MEMORANDUM FOR: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

FROM: André V. Mendes
Acting Chief Information Officer

ANDRE MENDES
Digitally signed by ANDRE MENDES
Date: 2019.09.25 16:55:07 +01'00'

SUBJECT: Department of Commerce Response to the FY 2019 OIG Draft Report: *The Department Needs to Improve Its Capability to Effectively Share Cyber Threat Information*

This memorandum transmits the Department of Commerce Office of the Chief Information Officer's response to the Office of the Inspector General's Draft Report: *The Department Needs to Improve Its Capability to Effectively Share Cyber Threat Information.*

DOC's Acting Chief Information Officer concurs with the findings and recommendations outlined in the subject report. The findings accurately reflect the period in which the inspection and testing was conducted. DOC has since remediated two of the findings and is in the process of documenting our remediation.

The DOC OCIO notes the challenges of its sharing capabilities, the accessibility of the Cyber Threat Intelligence Portal, and the policies, procedures, and training that needs to be put in place. Therefore, OCIO will continue to make changes to improve this program's procedures and security operations to ensure compliance of CISA requirements. Upon receipt of the OIG's final report, OCIO will provide a formal response within OIG's mandated time frame.

Please contact Donna Bennett, Deputy Chief Information Security Officer, at 202-482-5988, if you have any questions.

011200000334