Report No. DODIG-2019-016

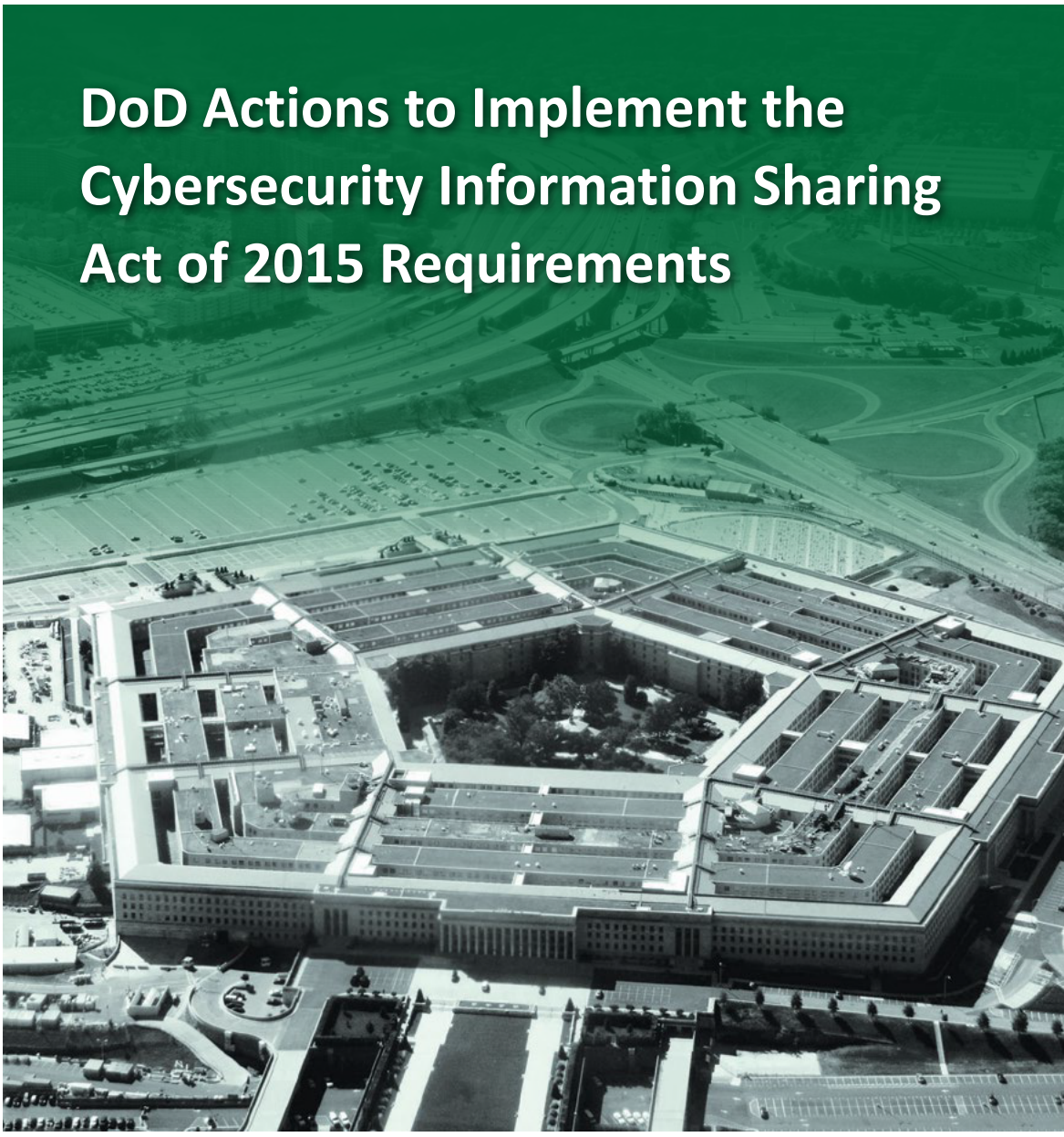
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

NOVEMBER 8, 2018

DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements



INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

Results in Brief

DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements

November 8, 2018

Objective

We determined whether the DoD took actions to implement the Cybersecurity Information Sharing Act of 2015 (CISA) requirements. Specifically, we assessed whether selected DoD Components:

- had sufficient policies and procedures in place for sharing cyber threat indicators or defensive measures with Federal and non-Federal entities;[1]
- verified the status of security clearances for private sector individuals authorized to share cyber threat indicators or defensive measures with the DoD;
- shared cyber threat indicators or defensive measures in a timely manner and removed irrelevant personally identifiable information (PII) when sharing the information with Federal and non-Federal entities; and
- assessed and mitigated barriers to sharing cyber threat indicators and defensive measures with Federal and non-Federal entities.

To accomplish our objective, we reviewed the policies and procedures in place for sharing both unclassified and classified

[1] CISA defines a cyber threat indicator as information that describes or identifies a malicious reconnaissance, a method of defeating a security control or exploitation of security vulnerability, or a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability. CISA also defines a defensive measure as an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or vulnerability.

Objective (cont'd)

cyber threat indicators and defensive measures and verified whether those policies and procedures were still current. We also reviewed select unclassified cyber threat indicators and defensive measures that were shared within the DoD, the Department of Homeland Security, and with private entities during 2016 to determine whether DoD officials complied with established policies and procedures as well as the CISA requirements. We obtained this information from four DoD Components—the National Security Agency (NSA), Defense Information Systems Agency (DISA), DoD Cyber Crime Center (DC3), and U.S. Cyber Command (USCYBERCOM).

Background

On December 18, 2015, the President signed CISA into law. According to Federal guidance, Congress designed CISA to encourage public and private sector entities to share cyber threat indicators and defensive measures while protecting classified information, intelligence sources and methods, and privacy.

Finding

The DoD took limited actions to implement the CISA requirements for sharing cyber threat indicators and defensive measures within the DoD and with other Federal and non-Federal entities. For example, the NSA and DC3 developed agency-level policies and procedures for sharing cyber threat indicators or defensive measures. The NSA, DISA, and DC3 timely shared cyber threat indicators or defensive measures within the DoD and with other Federal and non-Federal entities, and ensured that cyber threat indicator or defensive measure reports shared did not include irrelevant PII. However, none of the four DoD Components reviewed implemented all of the CISA requirements.

- DISA and USCYBERCOM did not have agency-level policies and procedures for sharing cyber threat indicators and defensive measures with Federal and non-Federal entities, as required by CISA.

Results in Brief

DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements

Finding (cont'd)

- DC3 did not verify whether 5 out of 32 nonstatistically sampled private sector individuals had an active security clearance before sharing cyber threat indicators and defensive measures in the Defense Industrial Base Network-Unclassified system. As a result, DC3 personnel removed 429 users from the system during the course of our audit.
- ~~(U//FOUO)~~ [redacted]

We determined that the four DoD Components did not implement all of the CISA requirements because the DoD Chief Information Officer (CIO) did not issue a DoD-wide policy on CISA implementation or require that the DoD Components comply with the CISA requirements. As a result, the DoD limited its ability to gain a more complete understanding of cybersecurity threats since it did not fully leverage the collective knowledge and capabilities of sharing entities, or disseminate internally generated cyber threat indicators and defensive measures with other Federal and non-Federal entities. Using the shared information, entities can improve their security posture by identifying affected systems, implementing protective measures, and responding to and recovering from incidents. This is critical because cyber attackers continually adapt their tactics, techniques, and procedures to evade detection, circumvent security controls, and exploit new vulnerabilities.

Recommendations

We recommend that the DoD CIO, in coordination with the Under Secretary of Defense for Policy, issue DoD-wide policy on CISA implementation, including a requirement for the DoD Components to document barriers to sharing cyber threat indicators and defensive measures and take appropriate actions to mitigate the identified barriers.

~~(U//FOUO)~~ We recommend that the Directors for the NSA and DC3 [redacted]

~~(U//FOUO)~~ We recommend that the DISA [redacted]

Management Comments and Our Response

~~(U//FOUO)~~ The Principal Deputy CIO, responding on behalf of the CIO, agreed to coordinate with the Under Secretary of Defense for Policy to issue DoD-Wide policy on the CISA implementation. The DISA Director and USCYBERCOM Commander both agreed [redacted] Therefore, those recommendations are resolved and will be closed once we verify that the agreed upon actions are implemented.

The Directors for the NSA and DC3 did not provide comments. Therefore, we request comments to the final report from the Directors of NSA, and DC3. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
DoD Chief Information Officer	None	1	None
Director, National Security Agency	2.a and 2.b	None	None
Director, Defense Information Systems Agency	None	3.a and 3.b	None
Director, DoD Cyber Crime Center	4.a and 4.b	None	None
Commander, U.S. Cyber Command	None	5.a and 5.b	None

Please provide Management Comments by December 10, 2018.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

November 8, 2018

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DOD CYBER CRIME CENTER
COMMANDER, U.S. CYBER COMMAND

SUBJECT: DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements (Report No. DODIG-2019-016)

We are providing this report for review and comment. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. The Principal Deputy Chief Information Officer responding on behalf of the Chief Information Officer agreed to Recommendation 1, the Defense Information Systems Agency Director agreed to Recommendations 3.a and 3.b, and the U.S. Cyber Command Commander agreed to Recommendations 5.a and 5.b; therefore, we do not require additional comments. However, the National Security Agency Director, and the DoD Cyber Crime Center Director did not respond to the draft report; therefore, we request that they provide comments to the final report by December 10, 2018.

Please send a PDF file containing your comments on the recommendations to audcso@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the cooperation and assistance received during the audit. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

Introduction

Objective

Our audit objective was to determine whether the DoD took actions to implement the Cybersecurity Information Sharing Act of 2015 (CISA) requirements.[2] Specifically, we assessed whether selected DoD Components:

- had sufficient policies and procedures for sharing cyber threat indicators or defensive measures with Federal and non-Federal entities;
- verified the status of security clearances for private sector individuals authorized to share cyber threat indicators or defensive measures with the DoD;
- shared cyber threat indicators or defensive measures in a timely manner and removed irrelevant personally identifiable information (PII) when sharing with Federal or non-Federal entities;[3] and
- assessed and mitigated barriers to sharing cyber threat indicators and defensive measures with Federal and non-Federal entities.

We focused this audit on the DoD Components that primarily shared cyber threat indicators and defensive measures—the National Security Agency (NSA), the Defense Information Systems Agency (DISA), the DoD Cyber Crime Center (DC3), and U.S. Cyber Command (USCYBERCOM).[4] See Appendix A for a discussion of the scope, methodology, and prior audit coverage.

Background

On December 18, 2015, the President signed CISA into law. According to Federal guidance, Congress designed CISA to create a cybersecurity information sharing process to encourage public and private sector entities to share cyber threat indicators and defensive measures while protecting classified information, intelligence sources and methods, and privacy.[5]

---

[2] Public Law 114-113, "Division N—Cybersecurity Act of 2015, Title I—Cybersecurity Information Sharing," December 18, 2015.

[3] We defined PII consistent with the definition in DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014. We defined "irrelevant PII" as PII that a Federal entity knows at the time of the sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat in accordance with CISA, section 103, "Sharing of Information by the Federal Government."

[4] We reviewed the policies and procedures in place to share cyber threat indicators and defensive measures during 2016 because the DoD Components under review provided responses based on those policies and procedures in the joint report provided to Congress in December 2017. We also reviewed select unclassified cyber threat indicators and defensive measures to determine whether officials complied with the established policies and procedures and the CISA requirements.

[5] "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016.

CISA's definition of a cyber threat indicator includes information that describes or identifies a malicious reconnaissance, a method of defeating a security control or exploitation of security vulnerability, or a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability.[6] Sharing cyber threat indicators provides access to threat information that might otherwise be unavailable to other organizations. Using shared resources, organizations can enhance their security posture by leveraging the knowledge, experience, and capabilities of their partners in a proactive way.

CISA's definition of a defensive measure includes an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or vulnerability.[7] An example of a defensive measure would be an action taken to block users from visiting a malicious domain by installing a website blocker application or configuring an existing blocker application.

CISA requires the Inspectors General of seven Federal entities—the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence—to jointly report to Congress no later than 2 years after the enactment date of CISA, and once every 2 years thereafter, on the actions of the Executive branch of the U.S. Government to carry out the CISA requirements.[8] Specifically, section 107, "Oversight of Government Activities," requires the Inspectors General, among other things, to:

- assess the sufficiency of policies, procedures, and guidelines relating to the sharing of cyber threat indicators within the Federal Government, including the removal of any personal information not directly related to cyber threat indicators or information that identifies a specific individual;
- assess whether the Federal entity properly classified cyber threat indicators or defensive measures and an accounting of the number of security clearances for individuals authorized by the Federal Government to share cyber threat indicators or defensive measures with the private sector;

[6] See the Glossary of this report for the full definition of a cyber threat indicator as defined by CISA.

[7] See the Glossary of this report for the full definition of a defensive measure as defined by CISA.

[8] CISA, section 102, "Definitions," identifies the seven Federal entities required to participate and section 107 requires the Inspectors Generals of those Federal entities to jointly report to Congress no later than 2 years after enactment of CISA and biennially thereafter.

- review the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under CISA, including a review of the appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures, and the timely and adequate sharing of cyber threat indicators or defensive measures with appropriate Federal and non-Federal entities;[9]
- assess the cyber threat indicators or defensive measures shared with the appropriate entities under CISA, among other things, including the number of cyber threat indicators or defensive measures shared and an assessment of any personal information not directly related to cyber threat indicators or information that identifies a specific individual that was shared in violation of CISA; and
- assess the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.[10]

Section 107 designates the Office of the Inspector General of the Intelligence Community (IC IG) as the lead agency for compiling the information from the seven Federal entities into a joint report. To meet the initial section 107 reporting requirement, the IC IG developed and provided a questionnaire to the Inspectors General of the seven Federal entities in February 2017. The questionnaire focused on the policies and procedures in place during 2016.[11] We forwarded the questionnaire and requested responses from the four DoD Components that primarily share cyber threat indicators and defensive measures within DoD and outside of the Department—the NSA, DISA, DC3, and USCYBERCOM. We provided the responses to the IC IG personnel, which incorporated them into the IC IG Report No. AUD-2017-005, "Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 19, 2017.

National Security Agency

The NSA leads the U.S. Government in cryptology that encompasses both signals intelligence and information assurance products and services, and enables computer network operations to gain an advantage for the Nation and our allies. The NSA collects, processes, analyzes, produces, and disseminates signals intelligence information and data under the authority of Executive Order 12333, National Security Directive 42, and DoD Directive 5100.20.[12] In response to a

[9] CISA does not define timeliness for sharing of cyber threat indicators or defensive measures.

[10] See Appendix B for the full citation of the CISA, section 107 joint reporting requirements.

[11] In addition to the six Departments, the IC IG also obtained the Office of the Director of National Intelligence's responses for the questionnaire and included the result in the "Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 19, 2017. See Appendix A for a link to the joint IC IG report.

[12] Executive Order 12333, "United States Intelligence Activities," December 4, 1981; National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990; and DoD Directive 5100.20, "National Security Agency/Central Security Service (NSA/CSS)," January 26, 2010.

January 2016 White House memorandum, the NSA started sending unclassified cyber threat indicators to the Department of Homeland Security (DHS) Automated Indicator Sharing (AIS) system.[13]

The AIS system is the U.S. Government's primary mechanism to exchange unclassified cyber threat indicators and defensive measures with the private sector. The system provides:

- the automated exchange of cyber threat indicators between and among Federal and non-Federal entities to allow participants to quickly mitigate cyber threats;
- a capability for participating organizations to connect to a DHS-managed system that allows bi-directional sharing of cyber threat indicators; and
- the enhanced ability to detect and block cyber adversaries before intrusions occur and identify ongoing cyber incidents.

Defense Information Systems Agency

~~(U//FOUO)~~ DISA is a combat support agency that provides information sharing capabilities to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of DoD operations. Since 2014, DISA has shared cyber threat indicators with 25 DoD and Federal entities using the Fight by Indicator (FbI) system. The FbI system provides the capability for cyberspace operations analysts to review cyber threat indicator reports and take further action, if necessary. [redacted]

Department of Defense Cyber Crime Center

DC3 is a DoD technical center for digital and multimedia forensics, cyber investigative training, technical solutions development for cybersecurity, and cyber analytics. As the DoD's operational focal point for the Defense Industrial Base (DIB) Cyber Security Program, DC3 receives cyber incident reports from defense contractors and voluntary private sector participants, analyzes the reports, and prepares cybersecurity information products to share with the Program participants for their cyber situational awareness and threat mitigation strategies.

[13] White House Memorandum 005632, "Participation in Automated Cyber Indicator Sharing with the Department of Homeland Security," January 15, 2016.

[14] ~~(U//FOUO)~~ [redacted]

DC3 shares unclassified cyber threat indicators and defensive measures with authorized system users through the DIB Network-Unclassified (DIBNet-U) portal, which enables secure voice and data transmission. DC3 also shares classified cyber threat information electronically with DIB participants through a secret-level web portal.[15] The DIBNet-U portal provides:

- an online application process for DIB companies to apply for the DIB Cyber Security Program;
- DIB Cyber Security Program and related information, and unclassified actionable threat information and document libraries;
- collaboration features, including a discussion forum and chat; and
- an incident reporting module.

DC3 also sends actionable unclassified cyber threat indicators, based on DIBNet-U reports, to the DHS AIS system.

U.S. Cyber Command

~~(U//FOUO)~~ USCYBERCOM unifies the direction of DoD cyberspace operations by focusing on three main areas: (1) defending the DoD information networks, (2) providing support to combatant commanders for execution of their missions around the world, and (3) strengthening the Nation's ability to withstand and respond to cyber attacks. USCYBERCOM shares classified cyber threat indicators within the DoD and with other Federal entities through secure phone, video teleconferencing, or e-mail; however, [redacted]

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[16] We identified that the DoD did not have internal controls over the sharing of cyber threat indicators and defensive measures as required by CISA or protect the DIBNet-U from unauthorized access. We will provide a copy of the report to the senior official responsible for internal controls for each of the DoD Components audited.

[15] DC3 defines authorized users as Government and private sector personnel who have been granted access to the DIBNet-U to share cyber threat indicators and defensive measures.

[16] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

The Cybersecurity Information Sharing Act of 2015 Was Inconsistently Implemented Across the DoD

The DoD took limited actions to implement the CISA requirements for sharing cyber threat indicators and defensive measures within the DoD and with other Federal and non-Federal entities. For example, the NSA and DC3 developed agency-level policies and procedures for sharing cyber threat indicators or defensive measures. The NSA, DISA, and DC3 timely shared cyber threat indicators or defensive measures within DoD and with other Federal and non-Federal entities, and ensured that cyber threat indicator or defensive measure reports did not include irrelevant PII. However, we also determined that none of the four DoD Components reviewed implemented all of the CISA requirements.

- DISA and USCYBERCOM did not have agency-level policies and procedures for sharing cyber threat indicators and defensive measures with Federal and non-Federal entities, as required by CISA.
- DC3 did not verify whether 5 out of 32 nonstatistically sampled private sector individuals had an active security clearance before sharing cyber threat indicators and defensive measures in the DIBNet-U system. As a result, DC3 personnel removed 429 users from the system in response to our finding.
- ~~(U//FOUO)~~ [redacted]

We determined that the four DoD Components did not implement all of the CISA requirements because the DoD Chief Information Officer (CIO) did not establish an overall DoD-wide policy for the implementation of CISA or require that the DoD Components comply with the CISA requirements. As a result, the DoD limited its ability to gain a more complete understanding of cybersecurity threats since it did not fully leverage the collective knowledge and capabilities of sharing entities, or disseminate internally generated cyber threat indicators and defensive measures to other Federal and non-Federal entities. Using the shared information, entities can improve their security posture by identifying affected systems, implementing protective measures, and responding to and recovering from incidents. This is critical because cyber attackers continually adapt their tactics, techniques, and procedures to evade detection, circumvent security controls, and exploit new vulnerabilities.

Cybersecurity Information Sharing Act of 2015 Implementation

Although the DoD initiated actions to implement the CISA requirements to share cyber threat indicators and defensive measures within the DoD and with other Federal and non-Federal entities, none of the four DoD Components reviewed implemented all of the CISA requirements.

Policies and Procedures

The NSA and DC3 had sufficient agency-level policies and procedures for sharing both unclassified and classified cyber threat indicators or defensive measures under CISA; however, DISA and USCYBERCOM did not. According to CISA, sharing guidance should include procedures to:

The NSA and DC3 had sufficient agency-level policies and procedures for sharing both unclassified and classified cyber threat indicators or defensive measures under CISA; however, DISA and USCYBERCOM did not.

- share cyber threat indicators and defensive measures in a timely manner;
- review cyber threat indicators for PII before sharing them;
- use and disseminate cyber threat indicators and defensive measures; and
- account for the number of security clearances for individuals authorized to share cyber threat indicators and defensive measures with the private sector.[17]

To determine whether the DoD Components had sufficient policies and procedures, we obtained agency-specific guidance relevant to cybersecurity information sharing. We considered the agency guidance sufficient if it contained specific procedures for:

- sharing, using, and disseminating cyber threat indicators and defensive measures in a timely manner;
- removing irrelevant PII;[18] and
- accounting for the security clearances of private sector individuals.

[17] See Appendix B for the full citation of the CISA, section 107 joint reporting requirements.

[18] We defined PII consistent with the definition in DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014. We defined "irrelevant PII" as PII that a Federal entity knows at the time of the sharing to be personal information or information that identifies a specific person not directly related to a cybersecurity threat in accordance with CISA, section 103, "Sharing of Information by the Federal Government."

Table 1 summarizes the sufficiency of each agency's policies or procedures.

Table 1. The Sufficiency of Policies or Procedures

Agency	Policies or Procedures Sufficient		
	Timely Sharing	Removing Irrelevant PII	Accounting for Security Clearance
NSA	Yes	Yes	N/A*
DISA	No	No	N/A*
DC3	Yes	Yes	Yes
USCYBERCOM	No	No	N/A*

* The NSA, DISA, and USCYBERCOM were not required to share cyber threat indicators and defensive measures with the private sector; therefore, there were no security clearances for the NSA, DISA, and USCYBERCOM to account for.

Source: The DoD OIG.

DISA guidance did not establish timeframes for the sharing of cyber threat indicators and defensive measures or require the removal of irrelevant PII. DISA personnel explained that they shared indicator reports from other DoD and Federal entities in accordance with DoD Instruction 8530.01.[19] The Instruction requires that DISA plan, mitigate, and execute DoD Information Network operations and Defensive Cyberspace Operations' internal measures at the DoD global and enterprise level. However, the Instruction did not establish timeframes for sharing cybersecurity information or specify controls over the publication and distribution of cyber threat information to prevent the improper disclosure of PII.

~~(U//FOUO)~~ USCYBERCOM did not establish timeframes for the sharing of cyber threat indicators and defensive measures or require the removal of irrelevant PII. [redacted][20] Although USCYBERCOM personnel relied on the cyber incident reporting timeframes and PII reporting guidelines identified in the manual, it does not provide guidelines specific to the sharing of cyber threat indicators and defensive measures in accordance with the CISA requirements.

[19] DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," July 25, 2017.

[20] Chairman of the Joint Chiefs of Staff Manual 6510.01B, "Cyber Incident Handling Program," July 10, 2012.

~~(U//FOUO)~~ Documented policies and procedures would provide additional assurance that DISA and USCYBERCOM will consistently share cyber threat indicators and defensive measures in accordance with the CISA requirements. Therefore, DISA and USCYBERCOM should [redacted]

Additionally, we recommend that the NSA and DC3 [redacted]

Verification of Security Clearances

DC3 did not verify whether 5 of 32 nonstatistically sampled private sector individuals had an active security clearance for authorized DIBNet-U system users prior to sharing cyber threat indicators and defensive measures in the system.[21] The NSA, DISA, and USCYBERCOM did not share cyber threat indicators or defensive measures directly with the private sector and thus, private sector personnel were not required to have security clearances to receive the information. However, DC3 requires that all DIBNet-U users have an active security clearance.[22] Therefore, we tested a sample of DIBNet-U users to determine whether they had an active security clearance.

DC3 did not verify whether 5 of 32 nonstatistically sampled private sector individuals had an active security clearance for authorized DIBNet-U system users prior to sharing cyber threat indicators and defensive measures in the system.

To determine whether DIBNet-U users had an active security clearance, we reviewed DC3 Access database used to maintain a current listing of active users and verified the security clearance information for selected users with the Joint Personnel Adjudication System (JPAS). This database had 881 active DIBNet-U users as of April 19, 2017. Our review identified discrepancies with the information contained in the database, such as users who had:

- an expired visitor access request to DC3 facility;
- no clearance level identified; or
- no visitor access request listed.

21 ~~(U//FOUO)~~ [redacted]

22 ~~(U//FOUO)~~ [redacted]

We obtained DC3's database of active users and judgmentally filtered the database to list only those users with the discrepancies listed above, which resulted in 290 of the 881 active DIBNet-U users. We then nonstatistically selected 32 of the 290 users and verified their security clearance information with JPAS. Of the 32 users nonstatistically sampled, 5 did not have the required security clearance in JPAS as shown in Table 2.

Table 2. Users Without an Active Security Clearance (as of April 19, 2017)

DIBNet-U User	Clearance Level on DC3's Record	Active Account on DIBNet-U	Expiration Date	Security Clearance in JPAS
1	Top Secret	Yes	2/25/2015	No active clearance
2	Not Listed	Yes	Not Listed	No record in JPAS
3	Not Listed	Yes	Not Listed	No active clearance
4	Top Secret	Yes	4/14/2015	No active clearance
5	Secret	Yes	6/29/2016	No active clearance

Source: The DoD OIG.

We notified DC3 officials of our results and they took immediate action to remove DIBNet-U access for the five users. DC3 officials stated that they also reviewed all of the DIBNet-U user accounts to determine the clearance status. Based on the review results, DC3 officials stated that they took the following actions:

- deactivated 429 of the 881 active DIBNet-U accounts for users that did not have an active clearance,
- created an updated database that shows a list of authorized users and the status of their account, the date visitor access requests are submitted, and the date the access request expires; and
- established a process to monitor the DIBNet-U user database for any discrepancies and take immediate action, when necessary.

Additionally, DC3 updated the DIBNet-U Operational Instruction to strengthen the controls over verifying the security clearances of DIBNet-U users. The Instruction now requires that the user support team record the JPAS clearance information in the DIBNet-U user database, run a daily query in the database for expired clearances, and update the database and deactivate the accounts with expired clearances in DIBNet-U.

Review of Cyber Threat Indicators and Defensive Measures for Timely Sharing and Irrelevant PII

~~(U//FOUO)~~ The NSA, DISA, and DC3 shared unclassified cyber threat indicators in a timely manner and without irrelevant PII. [redacted] and thus we excluded them from our review. CISA requires that Federal entities review whether cyber threat indicators and defensive measures were shared timely, and whether any information not directly related to a cybersecurity threat that is personal information of a specific individual was shared.

The NSA, DISA, and DC3 shared unclassified cyber threat indicators in a timely manner and without irrelevant PII.

Timely Sharing of Cyber Threat Indicators and Defensive Measures

~~(U//FOUO)~~ DC3 and DISA [redacted] Federal guidance states that Federal entities should make unclassified cyber threat indicators broadly available to each other and to non-Federal entities.[23] The guidance also states that a Federal entity must share cyber threat indicators with each appropriate Federal entity as quickly as operationally practicable, consistent with applicable law and the mission of those entities.

Removal of Irrelevant PII

The NSA, DISA, and DC3 ensured that cyber threat indicator or defensive measure reports shared with Federal entities or the private sector did not include irrelevant PII.

The NSA, DISA, and DC3 ensured that cyber threat indicator or defensive measure reports shared with Federal entities or the private sector did not include irrelevant PII. We reviewed a sample of unclassified cyber threat indicators and associated reports shared in 2016 to assess whether the DoD Components removed PII not directly related to a cyber threat indicator or defensive measure.

[23] "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016.

- ~~(U//FOUO)~~ For NSA, [redacted][24]
- ~~(U//FOUO)~~ For DISA, [redacted][25]
- ~~(U//FOUO)~~ For DC3, [redacted][26]

Barriers to Sharing Cyber Threat Indicators and Defensive Measures

All four DoD Components reviewed verbally stated that they had barriers to sharing cyber threat indicators when asked; however, none of them documented those barriers or identified plans to mitigate those barriers. CISA requires that Federal entities identify inappropriate barriers to sharing cyber threat indicators and defensive measures. The DoD Components provided us with the following barriers when asked.

All four DoD Components reviewed verbally stated that they had barriers to sharing cyber threat indicators when asked; however, none of them documented those barriers or identified plans to mitigate those barriers.

- NSA personnel stated that a barrier existed because they could not receive cyber threat indicators or defensive measures from the AIS system due to internal NSA storing procedures.[27]
- ~~(U//FOUO)~~ DISA personnel stated that a barrier existed because [redacted]
- DC3 personnel stated that they could not ensure that all DIB partners were actually reporting all cyber incidents to DC3, resulting in potentially incomplete information sharing.[28]

[24] For the NSA, we obtained 135 unclassified cyber threat indicator reports shared in 2016. We then nonstatistically selected 12 indicators for review.

[25] For DISA, we statistically selected the 45 of 68,165 cyber threat indicators shared in the FbI system for 2016. We then nonstatistically selected 10 of the 45 indicator reports for review.

[26] For DC3, we reviewed all 90 Incident Collection Format reports and 38 Customer Response Form reports shared in 2016. An Incident Collection Format report is for DIB participants to submit cyber security incidents through the DIBNet-U, and a Customer Response Form report contains a non-attributable summary of the incident as reported by the DIB partner.

[27] The AIS system is the U.S. Government's primary mechanism to exchange unclassified cyber threat indicators and defensive measures with the private sector.

[28] DC3 receives cyber incident reports from defense contractors and voluntary private sector participants, analyzes the reports, and prepares cybersecurity information products to share with the program participants for their cyber situational awareness and threat mitigation strategies. DC3 uses the DIBNet-U portal to share this communication.

- ~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ As a result, we recommend that the NSA, DISA, DC3, and USCYBERCOM [redacted]

No DoD-Wide Policy for Implementing CISA

The DoD CIO did not establish an overall DoD-wide policy for the implementation of CISA or require that the DoD Components comply with the CISA requirements. CISA requires that Federal entities submit a detailed report concerning the implementation of CISA that includes policies and procedures, real-time information sharing, an accounting of security clearances authorized to share cyber threat indicators or defensive measures with the private sector.

The DoD CIO did not establish an overall DoD-wide policy for the implementation of CISA or require that the DoD Components comply with the CISA requirements.

Additionally, DoD-wide policy outlining how DoD should implement the CISA requirements is needed because not all the CISA requirements are applicable to all of the DoD Components. For example, DC3 was the only DoD Component that accounted for security clearances since it shared cyber threat indicators and defensive measures with the private sector; whereas, the NSA and USCYBERCOM did not.[29]

To improve cybersecurity information sharing and to implement the CISA requirements within DoD, we recommend that the DoD CIO, in coordination with the Under Secretary of Defense for Policy, issue DoD-wide policy implementing the CISA requirements, including a requirement for DoD Components to document barriers to sharing cyber threat indicators and defensive measures and take appropriate actions to mitigate the identified barriers.

[29] DC3 verifies clearances before sharing classified information with the private sector through DIBNet-U.

The DoD Limited Its Ability to Share and Receive Cybersecurity Information

The inconsistent implementation of CISA by DoD Components limits DoD's ability to gain a more complete understanding of increasing and persistent cybersecurity threats by leveraging the collective knowledge and capabilities of sharing entities. The DoD can provide its Components, other Federal entities, and non-Federal entities access to cybersecurity information that might not be available to them by sharing cyber threat indicators and defensive measures. Using the shared information, entities can improve their security posture by identifying affected systems, implementing protective measures, and responding to and recovering from incidents. This is critical because cyber attackers continually adapt their tactics, techniques, and procedures to evade detection, circumvent security controls, and exploit new vulnerabilities.

The inconsistent implementation of CISA by DoD Components limits DoD's ability to gain a more complete understanding of increasing and persistent cybersecurity threats by leveraging the collective knowledge and capabilities of sharing entities.

According to Federal guidance, cybersecurity is one of the most important challenges we face as a Nation and a top priority of the Administration. A key element in the Government's efforts to address this threat is information sharing.[30] Improved sharing of cyber threat indicators and defensive measures would allow Federal and non-Federal entities to better understand the risks they face from adversaries. As such, the DoD should establish and maintain a framework for the cyber threat information sharing under CISA, considering factors such as the DoD Components' needs, capabilities, and unique restrictions.

As such, the DoD should establish and maintain a framework for the cyber threat information sharing under CISA, considering factors such as the DoD Components' needs, capabilities, and unique restrictions.

[30] White House Memorandum 005632, "Participation in Automated Cyber Indicator Sharing with the Department of Homeland Security," January 15, 2016.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Policy, issue DoD-wide policy implementing the Cybersecurity Information Sharing Act of 2015 requirements, including a requirement for the DoD Components to document barriers to sharing cyber threat indicators and defensive measures and take appropriate actions to mitigate the identified barriers.

Principal Deputy Chief Information Officer Comments

The Principal Deputy CIO, responding on behalf of the DoD CIO, agreed stating that the Office of the Chief Information Officer will coordinate with the Under Secretary of Defense for Policy to issue DoD-Wide policy on CISA implementation, requiring DoD Components to document barriers to sharing cyber threat indicators and defensive measures and actions taken to mitigate the identified barriers.

Our Response

Comments from the Principal Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify that the CIO issued CISA implementation policy and it includes a requirement for DoD Components to identify and mitigate any barriers for sharing cyber threat indicators and defensive measures.

Recommendation 2

We recommend that the Director, National Security Agency:

a. ~~**(U//FOUO)**~~ [redacted]

b. ~~(U//FOUO)~~ [redacted]

Management Comments Required

The National Security Agency Director did not respond to the recommendations; therefore, the recommendations are unresolved. We request that the Director provide comments on the final report.

Recommendation 3

We recommend that the Director, Defense Information Systems Agency:

a. ~~(U//FOUO)~~ [redacted]

b. ~~(U//FOUO)~~ [redacted]

Director, Defense Information Systems Agency

~~(U//FOUO)~~ The DISA Director agreed [redacted]

Our Response

~~(U//FOUO)~~ Comments from the DISA Director addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify that DISA [redacted]

~~(U//FOUO)~~ [redacted]

Recommendation 4

We recommend that the Director, DoD Cyber Crime Center:

a. ~~(U//FOUO)~~ [redacted].

b. ~~(U//FOUO)~~ [redacted]

Management Comments Required

The DoD Cyber Crime Center Director did not respond to the recommendations; therefore, the recommendations are unresolved. We request that the Director provide comments on the final report.

Recommendation 5

We recommend that Commander, U.S. Cyber Command:

a. ~~(U//FOUO)~~ [redacted]

b. ~~(U//FOUO)~~ [redacted]

Commander U.S. Cyber Command Comments

~~(U//FOUO)~~ The USCYBERCOM Commander agreed stating that USCYBERCOM will [redacted]

Our Response

~~(U//FOUO)~~ Comments from the USCYBERCOM Commander addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify that USCYBERCOM [redacted]

Appendix A

Scope and Methodology

We conducted this performance audit from March 2017 through September 2018 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish the audit objectives, we reviewed the policies and procedures in place during 2016 at the NSA, DISA, DC3, and USCYBERCOM for sharing both unclassified and classified cyber threat indicators and defensive measures and verified whether those policies and procedures were still current.[31] We also reviewed samples of unclassified cyber threat indicators and defensive measures that were shared within the DoD, the Department of Homeland Security, and with private entities during 2016 to determine whether DoD officials complied with established policies and procedures and the CISA requirements. We conducted site visits to DC3 in Linthicum, Maryland, as well as the NSA, DISA, and USCYBERCOM at Fort Meade, Maryland.

We analyzed DoD-wide and agency-level information sharing policies and procedures provided during the audit, such as:

- DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," July 25, 2017;
- Chairman of the Joint Chiefs Of Staff Manual 6510.01B, "Cyber Incident Handling Program," July 10, 2012;
- "DISA Cyberspace Defense Service Provider (CDSP) Standard Operating Procedure (SOP): DCC Countermeasures Procedures (Reporting, Collection, Review)," April 27, 2017;
- "DCISE Standard Operating Procedures, Incident Processing," May 20, 2016; and
- "NTOC Interim Procedures for Sharing CTIs with DHS for AIS," May 27, 2016.[32]

[31] For the initial biennial joint report to Congress, the IC IG decided to obtain 2016 data and information on the actions of the appropriate Federal entities to implement CISA, enacted in December 2015. For our audit, we validated the 2016 data and information obtained for the purposes of the joint report, which the IC IG issued in December 2017.

[32] DCISE stands for Defense Industrial Base (DoD-DIB) Collaborative Information Sharing Environment. NTOC stands for National Security Agency/Central Security Service Threat Operations Center.

We evaluated the DoD-wide and agency-level policies and procedures against Federal and DoD guidance, including:

- Public Law 114-113, "Division N—Cybersecurity Act of 2015, Title I—Cybersecurity Information Sharing," December 18, 2015;
- "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015," February 16, 2016; and
- DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013.

To test whether private sector DIBNet-U users had an active security clearance, we judgmentally selected users who had an expired clearance, had no clearance identified, or had no clearance expiration date listed; thereby reducing the total population of DIBNet-U authorized users from 881 to 290. We then nonstatistically selected 32 of the 290 users to determine whether the private sector users were a U.S. citizen and had an active DoD Secret-level security clearance as required to access the DIBNet-U.[33]

Use of Computer-Processed Data

We used computer-processed data from an NSA classified system, the DISA FbI system, and DC3 system to validate whether the DoD Components timely shared cyber threat indicators and defensive measures with other entities and removed irrelevant PII. The DoD Components provided a list of unclassified cyber threat indicators in an Excel spreadsheet or portable document format that were shared in 2016. We then used that data to generate a sample of cyber threat indicators and for each indicator, we analyzed the cyber threat indicator report with the shared cyber threat indicator to determine whether each agency removed irrelevant PII and timely shared the cyber threat indicator. The computer-processed data were used only to select samples for testing.

Additionally, we used computer-processed data from DC3's Access database to validate the security clearances of DIBNet-U system users. The system administrator provided a list of active users' data, in an Excel spreadsheet. We used the data to determine whether users had the required security clearance to access the system. To assess the reliability of the data, we selected a sample from the list and compared the sampled users' security clearances with the respective source data from JPAS. Therefore, we concluded that data were sufficiently reliable to support our findings, conclusions, and recommendations.

[33] ~~(U//FOUO)~~ [redacted]

Use of Technical Assistance

The DoD OIG Quantitative Methods Division provided assistance in developing the sampling methodology that we used to select samples for DIBNet-U users and the removal of irrelevant PII from the DISA and DC3 cyber threat indicator reports. Details are provided in the Scope and Methodology section and in the Finding.

Prior Coverage

During the last 5 years, the IC IG issued one report discussing CISA implementation. The report can be accessed at https://www.oversight.gov/report/icig/joint-report-implementation-cybersecurity-information-sharing-act-2015.

IC IG

Report No. AUD-2017-005, "Joint Report of the Implementation of the Cybersecurity Information Sharing Act of 2015," December 19, 2017

> The objective was to provide a joint report on actions taken in 2016 to carry out the CISA requirements. Each Office of Inspector General independently obtained the required assessments on its agency's implementation of the CISA requirements and provided the results to the IC IG. The results were summarized by the IC IG in the joint report provided to Congress.

Appendix B

CISA Requirements

CISA, section 102, "Definitions,"

> (3) Appropriate Federal Entities—The term ''appropriate Federal entities'' means the following:
>
> (A) The Department of Commerce,
>
> (B) The Department of Defense,
>
> (C) The Department of Energy,
>
> (D) The Department of Homeland Security,
>
> (E) The Department of Justice,
>
> (F) The Department of the Treasury, and
>
> (G) The Office of the Director of National Intelligence.

CISA, section 103, "Sharing of Information by the Federal Government,"

> (a) In General—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall develop and issue procedures to facilitate and promote—
>
> (1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of relevant entities and non-Federal entities that have appropriate security clearances;
>
> (2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level;
>
> (3) the timely sharing with relevant Federal entities and non-Federal entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators and defensive measures in the possession of the Federal Government;
>
> (4) the timely sharing with Federal entities and non-Federal entities, if appropriate, of information relating to cyber security threats or authorized uses under this title, in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats; and

(5) the periodic sharing, through publication and targeted outreach, of cybersecurity best practices that are developed based on ongoing analysis of cyber threat indicators, defensive measures, and information relating to cyber security threats or authorized uses under this title, in the possession of the Federal Government, with attention to accessibility and implementation challenges faced by small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)).

(b) Development of Procedures.

(1) In General—The procedures developed under sub-section (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators and defensive measures in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal entities and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying, in a timely manner, Federal entities and non-Federal 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 of the requirements of this title or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities sharing cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures;

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i.) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information not directly related to a cyber security threat that such Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(ii.) to implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual; and

(F) include procedures for notifying, in a timely manner, any United States person whose personal information is known or determined to have been shared by a Federal entity in violation of this title.

CISA, section 105, "Sharing of Cyber Threat Indicators and Defensive Measures with the Federal Government,"

(a) Requirement for Policies and Procedures.

(3) Requirements Concerning Policies and Procedures—Consistent with the guidelines required by subsection (b), the policies and procedures developed or issued under this subsection shall—

(A) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 104(c) through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are only subject to a delay, modification, or other action due to controls established for such real-time process that could impede real-time receipt by all of the appropriate Federal entities when the delay, modification, or other action is due to controls—

(I) agreed upon unanimously by all of the heads of the appropriate Federal entities;

(II) carried out before any of the appropriate Federal entities retains or uses the cyber threat indicators or defensive measures; and

(III) uniformly applied such that each of the appropriate Federal entities is subject to the same delay, modification, or other action; and (iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any non-Federal entity pursuant to section 104 in a manner other than the real-time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities; and

(C) ensure there are—

(i) audit capabilities; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner.

(b) Privacy and Civil Liberties.

(3) Content—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(E) Include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(c) Capability and Process Within the Department of Homeland Security.

(1) In General—Not later than 90 days after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any non-Federal entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title that are shared by a non-Federal entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) consistent with section 104, communications between a Federal entity and a non-Federal entity regarding a previously shared cyber threat indicator to describe the relevant cybersecurity threat or develop a defensive measure based on such cyber threat indicator; and

(ii) communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators and defensive measures shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by a non-Federal entity to any other non-Federal entity or a Federal entity, including cyber threat indicators or defensive measures shared with a Federal entity in furtherance of opening a Federal law enforcement investigation;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

CISA, section 107, "Oversight of Government Activities,"

(b) Biennial Report on Compliance.

(1) In General—Not later than 2 years after the date of the enactment of this Act, and not less frequently than once every 2 years thereafter, the Inspectors General of the appropriate Federal entities, in consultation with the Inspector General of the Intelligence Community and the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress an interagency report on the actions of the executive of the Federal Government to carry out this title during the most recent 2-year period.

(2) Contents—Each report submitted under paragraph (1) shall include, for the period covered by the report, the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines relating to sharing of cyber threat indicators within the Federal Government, including those policies, procedures, and guidelines relating the removal of information not directly related to a cybersecurity threat that is personal information of a specific or information that identifies a specific individual.

(B) An assessment of whether cyber threat indicators or defensive measures have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purpose of sharing cyber threat indicators or defensive measures with the private sector.

(C) A review of the actions taken by the Federal Government based on cyber threat indicators or defensive measures shared with the Federal Government under this title, including a review of the following:

(i). The appropriateness of subsequent uses and disseminations of cyber threat indicators or defensive measures.

(ii) Whether cyber threat indicators or defensive measures were shared in a timely and adequate manner with appropriate entities, or, if appropriate, were made publicly available.

(D) An assessment of the cyber threat indicators or defensive measures shared with the appropriate Federal entities under this title, including the following:

(i) The number of cyber threat indicators or defensive measures shared through the capability and process developed under section 105(c).

(ii) An assessment of any information not directly related to a cybersecurity threat that is personal information of a specific individual or information identifying a specific individual and was shared by a non-Federal government entity with the Federal government in contravention of this title, or was shared within the Federal Government in contravention of the guidelines required by this title, including a description of any significant violation of this title.

(iii) The number of times, according to the Attorney General, that information shared under this title was used by a Federal entity to prosecute an offense listed in section 105(d)(5)(A).

(iv) A quantitative and qualitative assessment of the effect of the sharing of cyber threat indicators or defensive measures with the Federal Government on privacy and civil liberties of specific individuals, including the number of notices that were issued with respect to a failure to remove information not directly related to a cybersecurity threat that was personal information of a specific individual or information that identified a specific individual in accordance with the procedures required by section 105(b)(3)(E).

(v) The adequacy of any steps taken by the Federal Government to reduce any adverse effect from activities carried out under this title on the privacy and civil liberties of United States persons.

(E) An assessment of the sharing of cyber threat indicators or defensive measures among Federal entities to identify inappropriate barriers to sharing information.

(3) Recommendations—Each report submitted under this subsection may include such recommendations as the inspectors general may have for improvements or modifications to the authorities and processes under this title.

(c) Independent Report on Removal of Personal Information—Not later than 3 years after the date of the enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this title. Such report shall include an assessment of the sufficiency of the policies, procedures, and guidelines established under this title in addressing concerns relating to privacy and civil liberties.

(d) Form of Reports—Each report required under this section shall be submitted in an unclassified form, but may include a classified annex.

(e) Public Availability of Reports—The unclassified portions of the reports required under this section shall be made available to the public.

Management Comments

DoD Principal Deputy Chief Information Officer

CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

OCT 12 2018

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment on DoD Inspector General Proposed Report, "DoD Actions Taken to Implement the Cybersecurity Information Sharing Act of 2015 Requirements," (D2017-D00RB-0094.000)

Contained herein is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General (IG) Proposed Report, "DoD Actions Taken to Implement the Cybersecurity Information Sharing Act (CISA) of 2015 Requirements," (D2017-D000RB-0094.000).

DoD IG RECOMMENDATION: The DoD CIO in coordination with the Under Secretary of Defense for Policy (USD(P)), issue a DoD-wide policy on CISA implementation, including a requirement for DoD Components to document barriers to sharing cyber threat indicators and defensive measures and take appropriate actions to mitigate the identified barriers.

DoD CIO RESPONSE: DoD CIO agrees with the DoD IG recommendation. The DoD CIO will coordinate with the USD(P) to issue DoD-wide policy on CISA implementation, including a requirement for DoD Components to document barriers to sharing cyber threat indicators and defensive measures and take appropriate actions to mitigate the identified barriers.

A security review to verify "FOR OFFICIAL USE ONLY" (FOUO) markings in the report has been completed and there are no additional recommendations.

The point of contact for this matter is [redacted].

Essye B. Miller
Principal Deputy

Director, Defense Information Systems Agency

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

MEMORANDUM FOR DOD INSPECTOR GENERAL

SUBJECT: Follow-up Audit: DoDIG Draft Report - DoD Actions to Implement CISA of 2015 Requirements (D2017-D000RB-0094.000)

The following comments depict our position regarding the DoDIG Draft Report:

a) Recommendation 3a – Concur with Comment

i) [redacted]

(a) Action: Complete

[redacted]

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Director, Defense Information Systems Agency (cont'd)

DISA Memo, ID6, Follow-up Audit: DoDIG Draft Report - DoD Actions to Implement CISA of 2015 Requirements (D2017-D000RB-0094.000)

(a) Action: Complete

[redacted]

b) Recommendation 3b – Concur

i) [redacted]

(2) [redacted]

Please contact [redacted], or [redacted] should you have any questions.

Nancy A Norton

NANCY A. NORTON
Vice Admiral, USN
Director

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

2

Commander, U.S. Cyber Command

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

DEPARTMENT OF DEFENSE
UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

OCT 2 2 2018

Reply to:
Commander

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL

Subject: [redacted]

[redacted]

3. (~~U//FOUO~~) My Point of Contact for this action is [redacted], USCYBERCOM J33, [redacted]

PAUL M. NAKASONE
General, U.S. Army
Commander

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Acronyms and Abbreviations

AIS	Automated Indicator Sharing
CIO	Chief Information Officer
CISA	Cybersecurity Information Sharing Act
DC3	DoD Cyber Crime Center
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DIBNet-U	Defense Industrial Base Network-Unclassified
DISA	Defense Information Systems Agency
FbI	Fight by Indicator
IC IG	Office of the Inspector General of the Intelligence Community
JPAS	Joint Personnel Adjudication System
NSA	National Security Agency
NTOC	NSA Threat Operations Center
PII	Personally Identifiable Information
USCYBERCOM	U.S. Cyber Command

Glossary

Automated Indicator Sharing. The DHS's Automated Indicator Sharing initiative, which includes a technical system that enables automated, bi-directional, cyber threat indicator and defensive measure sharing between AIS system participants and Federal entities, through the National Cybersecurity and Communications Integration Center. The AIS system serves as the real-time process described in section 105(c) of the CISA (Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Division N, Title I) for sharing cyber threat indicators and measures between AIS system participants and Federal entities.

Cybersecurity Threat. An action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system; but does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cyber Threat Indicator. Information that is necessary to describe or identify:

- malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
- a method of defeating a security control or exploitation of a security vulnerability;
- a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
- a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
- malicious cyber command and control;
- the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
- any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
- any combination thereof.

~~(U//FOUO)~~ Defense Industrial Base Network. DC3 shares cyber threat indicators and defensive measures through the DIBNet portal. The DIBNet portal enables secure voice and data transmission among authorized system users. The DIBNet portal provides an online application process for DIB companies to apply to join the program; [redacted] unclassified actionable threat information; document libraries; and collaboration features, including a discussion forum, chat, and incident-reporting module.

Defensive Measure. An action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

DoD Information Network. The set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

Federal Entity. A department or agency of the United States or any component of such department or agency.

Fight by Indicator. DISA shares cyber threat indicators and defensive measures through its Cyber Situational Awareness Analytics Capabilities FbI system, which provides Enterprise Defensive Cyberspace Operations Analysts with the ability to automate Defensive Cyber Operations workflows, including indicator extraction, indicator database functions, and countermeasure functionality. This data is used for standardized and unique reporting functionality, enhanced sorting and tagging capabilities, and generating and tracking countermeasures workflow.

Malicious Cyber Command and Control. A method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

Malicious Reconnaissance. A method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

Non-Federal Entity. Any private entity, non-Federal Government agency or department, or State, tribal, or local government (including a political subdivision, department, or agency thereof); but does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

Personally Identifiable Information. Information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information. PII also includes personal information and information in identifiable form.

Private Entity. Any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer employee, or agent thereof; includes a State, tribal, or local government performing utility services, such as electric, natural gas, or water services.

Private Sector. An umbrella term that may be applied to any or all of the nonpublic or commercial individuals and businesses, specified nonprofit organizations, most of academia and other scholastic institutions, and selected nongovernmental organizations.

Security Vulnerability. Any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Signals Intelligence. A category of intelligence comprising, either individually or in combination, all communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted; and intelligence derived from communications, electronic, and foreign instrumentation signals.

Signature. A recognizable, distinguishing pattern associated with an attack, such as a binary string in a virus or a particular set of keystrokes used to gain unauthorized access to a system.

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible waste, fraud, and abuse in government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098