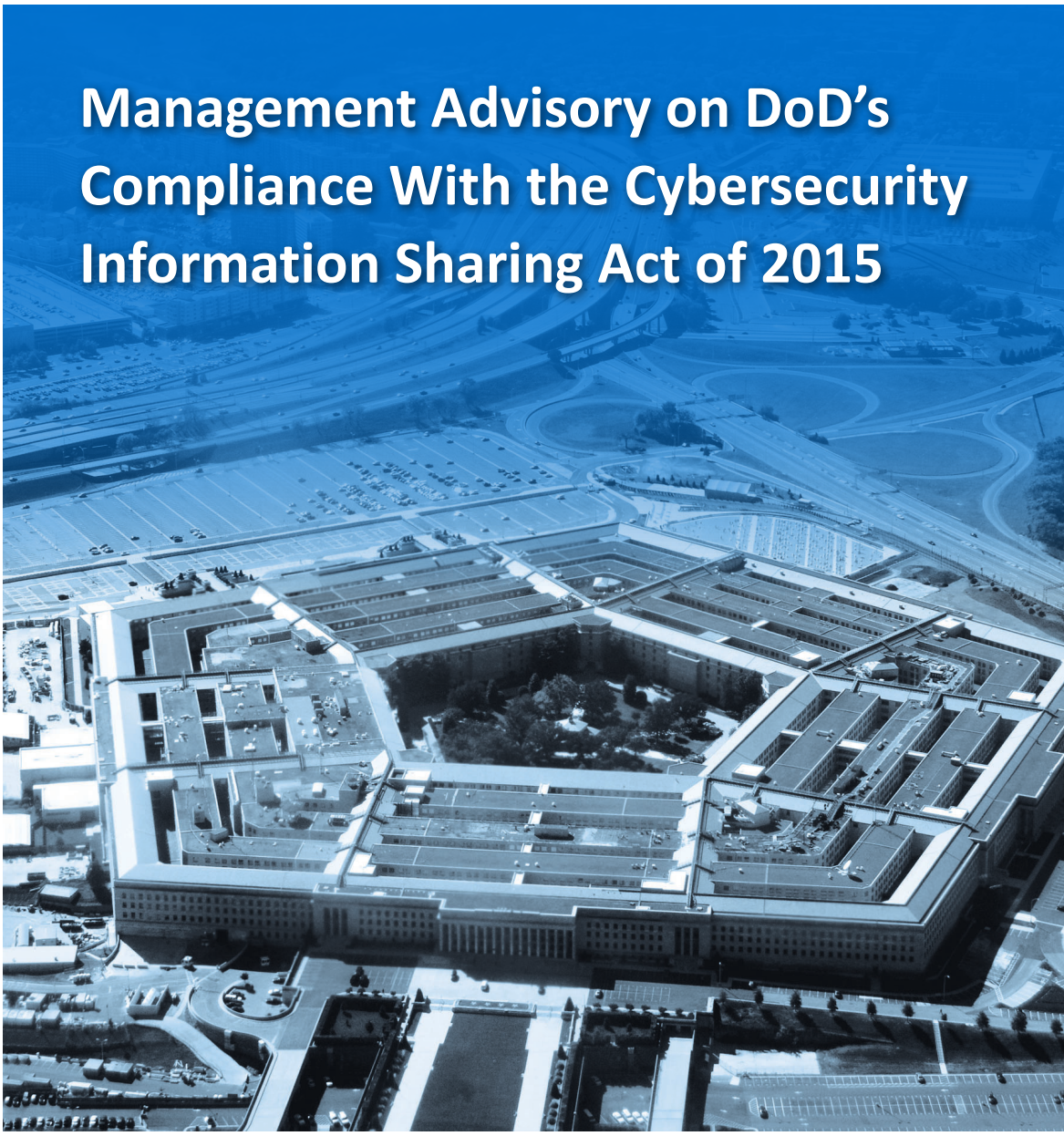
Report No. DODIG-2022-092

INSPECTOR GENERAL

U.S. Department of Defense

MAY 10, 2022

Management Advisory on DoD's Compliance With the Cybersecurity Information Sharing Act of 2015



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

May 10, 2022

MEMORANDUM FOR DIRECTOR, DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY

SUBJECT: Management Advisory on DoD's Compliance With the Cybersecurity Information Sharing Act of 2015 (Report No. DODIG-2022-092)

The purpose of this management advisory is to provide the status of DoD's compliance with the Cybersecurity Information Sharing Act of 2015 (CISA). CISA requires the Inspectors General of seven Federal agencies, including the DoD, to jointly report to Congress every 2 years on the actions taken by the Executive branch to implement CISA requirements. We assessed the DoD's actions taken to implement CISA and provided our results to the Intelligence Community Inspector General, who issued an interagency report to Congress on December 2, 2021, summarizing the assessment results for all seven Federal agencies. Because that report, AUD-2021-002, "Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 2, 2021, did not include recommendations, we are issuing this management advisory to report the DoD-specific assessment results and issue recommendations for corrective action. We conducted the assessment with integrity, objectivity, and independence, as required by the Council of Inspectors General for Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General.

We provided a draft copy of this management advisory to DoD management and requested written comments on the findings and recommendations. We considered management's comments on the draft when preparing the final management advisory.

This management advisory contains four recommendations that we consider resolved but open. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this advisory, the recommendations will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, we will close the recommendations. Please provide us within 90 days documentation showing that the agreed-upon actions are complete. Send

your response as a PDF file to followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

We appreciate the cooperation and assistance received during the assessment. Please direct questions to me at [redacted]

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Background

On December 18, 2015, the "Consolidated Appropriation Act, 2016," including the "Cybersecurity Information Sharing Act of 2015," became law.[1] The Cybersecurity Information Sharing Act (CISA) was established to improve cybersecurity in the United States by creating a framework to facilitate and promote the sharing of cyber threat information among and between Federal and non-Federal agencies. To comply with CISA, Federal agencies must develop procedures related to the sharing of cyber threat indicators (CTIs) and defensive measures, as well as the removal of personally identifiable information from shared CTIs and defensive measures.[2]

CTIs include threat-related information such as methods of defeating or causing users to unwittingly enable the defeat of security controls and methods of exploiting security vulnerabilities. Defensive measures are the actions, devices, procedures, techniques, or other measures 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.

CISA requires the Inspectors General of seven Federal agencies, including the DoD, to jointly report to Congress every 2 years on the actions taken by the Executive branch to implement CISA. We assessed the DoD actions taken to implement CISA and provided our assessment results to the Intelligence Community Inspector General, who is responsible for reporting the results from the seven Inspectors General to Congress. The Intelligence Community Inspector General issued an interagency report to Congress on December 2, 2021, which included our assessment of the following eight DoD Components.[3]

U.S. Cyber Command

The U.S. Cyber Command is a combatant command that defends DoD information networks, provides support to combatant commanders, and strengthens the DoD's ability to withstand and respond to cyber attacks. The command also works to improve the DoD's capabilities to operate resilient and reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace.

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

[2] We refer to CTIs and defensive measures collectively as cyber threat information.

[3] Intelligence Community Inspector General Report No. AUD-2021-002, "Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 02, 2021. This report can be accessed at the oversight.gov website.

National Security Agency

The National Security Agency is a combat support agency that leads the U.S. Government in cryptology for signal intelligence and cybersecurity products and services. The agency enables computer network operations to gain an advantage for the United States against its adversaries.

Defense Information Systems Agency

The Defense Information Systems Agency (DISA) is a combat support agency that plans, engineers, tests, fields, and operates information sharing capabilities for joint warfighters, national-level leaders, and other mission and coalition partners.[4]

Defense Intelligence Agency

The Defense Intelligence Agency (DIA) is a combat support agency that produces, analyzes, and shares military intelligence to Service members and defense policymakers. The DIA serves as the U.S. primary manager and producer of foreign military intelligence. The DIA produces and manages intelligence for the Secretary of Defense, Joint Chiefs of Staff, and Unified Combatant Commands.

National Reconnaissance Office

The National Reconnaissance Office (NRO) designs, builds, launches, and maintains intelligence satellites. The NRO provides global communications, precision navigation, early warning of missile launches, signals intelligence, and near real-time imagery.

National Geospatial-Intelligence Agency

The National Geospatial-Intelligence Agency (NGA) is a combat support agency that provides geospatial intelligence for U.S. security. The NGA leads the U.S. Government in managing, monitoring, and analyzing imminent threats and reports those threats to national decision makers.

Defense Counterintelligence and Security Agency

The Defense Counterintelligence and Security Agency (DCSA) provides security and counterintelligence support services to the DoD and law enforcement, Intelligence Community partners, and cleared contractors. The DCSA performs background investigations on individuals who work for the Executive branch and other branches of the Government to ensure the trustworthiness of the U.S. Government's workforce; the integrity of its cleared contractor support; and the nature of its technologies, services, and supply chains.

[4] The DISA Director is dual-hatted as the Commander of Joint Force Headquarters–DoD Information Network. Therefore, DISA manages the cyber threat system that the Joint Force Headquarters–DoD Information Network uses to send, receive, and analyze CTIs.

DoD Cyber Crime Center

The DoD Cyber Crime Center is a DoD cyber center for digital and multimedia forensic services, cyber technical training, vulnerability sharing, and cyber analytics. The center is also the operational focal point for Defense Industrial Base cybersecurity in which it analyzes, produces, and distributes cyber products that contain actionable cyber threat information to stakeholders in the DoD, U.S. Government, and Defense Industrial Base.

Assessment Methodology

We assessed DoD actions taken in 2019 and 2020 to implement CISA. Specifically, we reviewed the eight DoD Components' responses to 30 questions that the Intelligence Community Inspector General developed concerning CISA. The questions focused on the following five areas.

- Policies and procedures for sharing CTIs
- Classification of CTIs and defensive measures shared with the private sector
- Use and disseminate CTIs or defensive measures
- Protection of individuals' privacy and civil liberties when sharing CTIs
- Potential barriers to, and best practices for, sharing CTIs and defensive measures

This management advisory focuses on the areas in which the DoD Components did not adequately implement CISA requirements. For more information regarding DoD's specific responses to the 30 questions and the DoD Components' compliance with CISA, see the interagency joint report.[5]

[5] Intelligence Community Inspector General Report No. AUD-2021-002, "Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 02, 2021. This report can be accessed at the oversight.gov website.

DoD Compliance With CISA

The DoD Components met CISA requirements for four of the five areas we reviewed; however, four of the eight DoD Components—DISA, DIA, NGA, and DCSA—did not have sufficient policies or procedures for sharing CTIs as required by CISA Section 103(a) and (b) and Section 105(a) and (b). See the Appendix for the full content of those CISA sections. The DoD OIG addressed the lack of a DoD-wide policy for sharing CTIs in an audit report issued in November 2018.[6] In that report, the DoD OIG recommended that the DoD Chief Information Officer issue DoD-wide policy for sharing CTIs.

The DoD Chief Information Officer agreed to the recommendation and sent a draft of the policy to the DoD Components for comment but did not establish a final issuance date. On January 17, 2019, the DoD Chief Information Officer issued interim guidance that required the U.S. Cyber Command, National Security Agency, DISA, and DoD Cyber Crime Center to issue internal procedures for sharing CTIs until the DoD-wide policy was issued. However, the interim guidance did not include a requirement for the DIA, NGA, NRO, and DCSA to issue internal procedures.[7]

For this audit, we reviewed the policies and procedures for all eight DoD Components that share CTIs. DISA, DIA, DCSA, and NGA internal procedures lacked one or more of the CISA policy requirements. Specifically,

- DISA's draft procedures document, "Joint Force Headquarters–DoD Information Network/Defense Information Systems Agency Cyber Threat Information Sharing Policy Implementation and Capability Procedures Document," did not include guidance for removing personal information from CTIs; notifying individuals if personal information was shared in a CTI or defensive measure; notifying Federal agencies that they received CTIs with known errors; or identifying security controls to protect against unauthorized access to CTIs and defensive measures.
- DIA's "Incident Response Team Standard Operating Procedure," June 17, 2019, did not include guidance for removing personal information from CTIs; notifying individuals if personal information was shared in a CTI or defensive measure; or notifying Federal agencies that they received CTIs with known errors.
- DCSA's "Enterprise Incident Response Plan Standard Operating Procedure," July 20, 2020, did not include guidance for removing personal information from CTIs; notifying individuals if personal information was shared in a CTI or defensive measure; or notifying Federal agencies that they received CTIs with known errors.

[6] Report No. DODIG-2019-016, "DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements," November 8, 2018.

[7] The prior audit generally focused on DoD Components that shared unclassified CTIs, subsequent CISA audits included DoD Components that share classified and unclassified CTIs.

- NGA's "Cyber Threat Intelligence Program Standard Operating Procedure," January 22, 2021, did not include guidance for notifying Federal agencies that they received CTIs with known errors.

Although the DoD Chief Information Officer plans to issue CISA policy, it is important that the DoD Components have internal procedures to ensure compliance with CISA. Therefore, until the DoD Chief Information Officer issues DoD-wide policy, the DoD Components should use the guidance contained in the following four documents developed by the Office of the Director of National Intelligence, the Department of Homeland Security, the DoD, and the Department of Justice to establish those internal procedures.

- Department of Homeland Security and Department of Justice, "Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government," June 15, 2016, establishes procedures for receiving, handling, and disseminating CTIs shared with the Department of Homeland Security by all Federal agencies under CISA.
- Department of Homeland Security and Department of Justice, "Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015," June 15, 2018, establishes privacy and civil liberties guidelines for receiving, retaining, using, and disseminating CTIs by a Federal agency under CISA.
- Department of Homeland Security and Department of Justice, "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," October 2020, helps non-Federal agencies identify and share CTIs with Federal agencies under CISA.
- Office of the Director of National Intelligence, the Department of Homeland Security, the DoD, and the Department of Justice, "Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015," February 16, 2016, provides procedures for Federal agencies to share cyber threat information with non-Federal agencies.

Recommendations, Management Comments, and Our Response

Redirected and Renumbered Recommendations

As a result of management comments, we redirected Recommendation 1 from the Joint Force Headquarters–DoD Information Network Chief Data Officer to the Joint Force Headquarters–DoD Information Network Chief of Staff. We also removed Recommendation 3 because we verified that the NRO had sufficient policies and procedures in place for sharing cyber threat indicators prior to the date we issued the draft management advisory. Therefore, we renumbered draft Recommendation 4 as Recommendation 3 and Recommendation 5 as Recommendation 4.

Recommendation 1

We recommend that the Joint Force Headquarters–DoD Information Network Chief of Staff, in coordination with the Defense Information Systems Agency Chief Information Officer, update and issue the "Joint Force Headquarters–DoD Information Network/Defense Information Systems Agency Cyber Threat Information Sharing Policy Implementation and Capability Procedures Document," ensuring it includes:

a. **Guidance for removing personal information or information that identified an individual from cybersecurity threats.**

b. **Procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.**

c. **Guidance to identify the security controls to protect against unauthorized access to or acquisition of the cyber threat indicators and defensive measures shared.**

d. **Procedures for notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure.**

Joint Force Headquarters–DoD Information Network Comments

The Joint Force Headquarters-DoD Information Network Chief of Staff agreed, stating that Joint Force Headquarters-DoD Information Network will update its internal procedures to incorporate the recommendation by June 20, 2022. The Chief of Staff stated that the procedures would also address the minimization of classified material across their systems, as practicable. The Chief of Staff also stated that Joint Force Headquarters-DoD Information Network follows internal processes to remove personal individual information from cybersecurity threat information unless specifically required by DoD policy to share that information with a mission partner. In those instances, Joint Force Headquarters-DoD Information Network shares the information using the appropriate channels.

Our Response

Comments from the Chief of Staff addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Chief of Staff provides documentation showing that the internal procedures were updated and issued.

Recommendation 2

We recommend that the Defense Intelligence Agency Chief Information Security Officer update and reissue the "Incident Response Team Standard Operating Procedure," June 17, 2019, ensuring it includes:

a. **Guidance for removing personal information or information that identified an individual from cybersecurity threats.**

b. Procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.

c. Procedures for notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure.

Defense Intelligence Agency Comments

The DIA Chief Information Officer Operation Branch Chief for the Cyber and Security Division, responding for the DIA Chief Information Security Officer, agreed, stating that the DIA Computer Network Defense Center will update the DIA's internal procedures to incorporate the recommendation. The Operation Branch Chief also provided a copy of the updated draft guidance.

Our Response

Comments from the Operation Branch Chief addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Operation Branch Chief provides documentation showing that the internal procedures were finalized and issued.

Recommendation 3

We recommend that the Defense Counterintelligence and Security Agency Chief Information Security Officer update and reissue the "Enterprise Incident Response Plan Standard Operating Procedure," July 20, 2020, ensuring it includes:

a. Guidance for removing personal information or information that identified an individual from cybersecurity threats.

b. Procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.

c. Procedures for notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure.

Defense Counterintelligence and Security Agency Comments

The DCSA Designated Authorizing Official, responding for the DCSA Chief Information Security Officer, agreed, stating that the DCSA will update the DCSA Enterprise Incident Response Plan to incorporate our recommendations by July 1, 2022.

Our Response

Comments from the Designated Authorizing Official addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Designated Authorizing Official provides documentation showing that the DCSA Enterprise Incident Response Plan was updated and issued.

Recommendation 4

We recommend that the Director, Cybersecurity Operations Center, National Geospatial-Intelligence Agency, update and reissue the "Cyber Threat Intelligence Program Standard Operating Procedure" January 22, 2021, ensuring it includes procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.

National Geospatial-Intelligence Agency Comments

The NGA Director for the Cybersecurity Operations Center agreed, stating that the NGA will update and reissue the Cyber Threat Intelligence Program Standard Operating Procedure incorporating our recommendation.

Our Response

Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the Director provides documentation showing that the Cyber Threat Intelligence Program Standard Operating Procedure were updated and issued.

Appendix

CISA Requirements

CISA states that 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 jointly develop and issue procedures to facilitate and promote:[8]

> (1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal 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 cybersecurity 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 analyses 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, 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)).

[8] Public Law 114-113, "Division N—Cybersecurity Act of 2015, Title I—Cybersecurity Information Sharing," December 18, 2015, Section 103, "Sharing of Information by the Federal Government."

(b) DEVELOPMENT OF PROCEDURES.

(1) IN GENERAL.-The procedures developed under subsection (a) shall:

(A) ensure the Federal Government has and maintain 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;

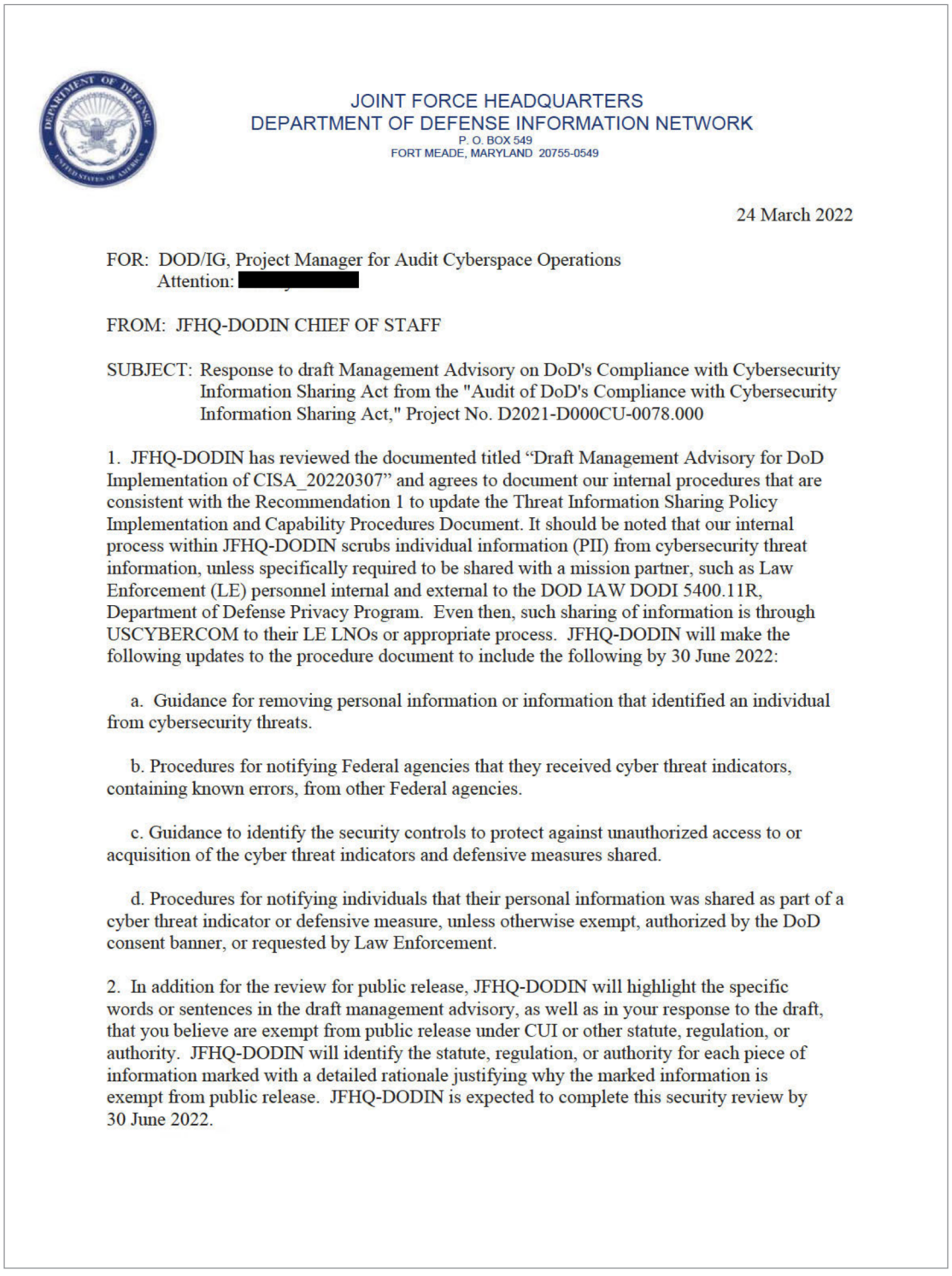
(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator: (i)to review such cyber threat indicator to assess whether such cyber threat indicator contains any information, not directly related to a cybersecurity threat, that such Federal entity knows at the 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.

(2) CONSULTATION.-In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall consult with appropriate Federal entities, including the Small Business Administration and the National Laboratories (as defined in section 2 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

Management Comments

Joint Force Headquarters–DoD Information Network



JOINT FORCE HEADQUARTERS
DEPARTMENT OF DEFENSE INFORMATION NETWORK
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

24 March 2022

FOR: DOD/IG, Project Manager for Audit Cyberspace Operations
Attention: [redacted]

FROM: JFHQ-DODIN CHIEF OF STAFF

SUBJECT: Response to draft Management Advisory on DoD's Compliance with Cybersecurity Information Sharing Act from the "Audit of DoD's Compliance with Cybersecurity Information Sharing Act," Project No. D2021-D000CU-0078.000

1. JFHQ-DODIN has reviewed the documented titled "Draft Management Advisory for DoD Implementation of CISA_20220307" and agrees to document our internal procedures that are consistent with the Recommendation 1 to update the Threat Information Sharing Policy Implementation and Capability Procedures Document. It should be noted that our internal process within JFHQ-DODIN scrubs individual information (PII) from cybersecurity threat information, unless specifically required to be shared with a mission partner, such as Law Enforcement (LE) personnel internal and external to the DOD IAW DODI 5400.11R, Department of Defense Privacy Program. Even then, such sharing of information is through USCYBERCOM to their LE LNOs or appropriate process. JFHQ-DODIN will make the following updates to the procedure document to include the following by 30 June 2022:

a. Guidance for removing personal information or information that identified an individual from cybersecurity threats.

b. Procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.

c. Guidance to identify the security controls to protect against unauthorized access to or acquisition of the cyber threat indicators and defensive measures shared.

d. Procedures for notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure, unless otherwise exempt, authorized by the DoD consent banner, or requested by Law Enforcement.

2. In addition for the review for public release, JFHQ-DODIN will highlight the specific words or sentences in the draft management advisory, as well as in your response to the draft, that you believe are exempt from public release under CUI or other statute, regulation, or authority. JFHQ-DODIN will identify the statute, regulation, or authority for each piece of information marked with a detailed rationale justifying why the marked information is exempt from public release. JFHQ-DODIN is expected to complete this security review by 30 June 2022.

Joint Force Headquarters–DoD Information Network (cont'd)

3. Here are a few changes requested with your draft report.

a. JFHQ-DODIN is a subordinate command to United States Cyber Command (USCYBERCOM) and follows reporting and sharing information guidance from USCYBERCOM. As an operational headquarters, we take direction from USCYBERCOM and not DISA. DISA performs similar functions as do services, in the support of a joint command, to JFHQ-DODIN. Therefore, our internal processes for operational reporting and information sharing are different than DISA as we do not report to DOD CIO.

b. The document references the Joint Force Headquarters–DoD Information Network Chief Data Officer (CDO), please replace title with Chief of Staff as there is no CDO position at JFHQ-DODIN.

c. As noted above, our internal processes are aligned to DODI 5400.11. We minimize any PII to the maximum extent practicable. DODI 5400.11R provides the blanket routine use for law enforcement (Appendix 3, section AP3.1.) that applies to all DoD Component systems notices and is also part of the DOD Consent Banner. This permits Components, on their own initiative, to report indications of violations of law found in a system of records to a law enforcement activity.

d. Finally, DODI 5400.11R, paragraph C5.1.3., states component rules shall include a blanket exemption for Classified Material. Our process, once documented, will address the minimization across all of our systems, as practicable.

4. If there are any questions regarding this response, then please contact [redacted]

HOWE.BRYCE.E RIC[redacted]

BRYCE E. HOWE
Chief of Staff

Defense Intelligence Agency

~~Classification: UNCLASSIFIED//FOUO~~

DEFENSE INTELLIGENCE AGENCY
200 MACDILL BOULEVARD
BUILDING 6000
WASHINGTON, D.C. 20340-5100
[redacted]

[redacted] March 28, 2022

(U) To: INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

(U) SUBJECT: DIA Response to Inspector General (IG) Memorandum, "Management Advisory on DoD's Compliance with Cybersecurity Information Sharing Act of 2015" (Project No. D2021-D000CU-0078.001)

(U) Reference: a. Management Advisory on DoD's Compliance With Cybersecurity Information Sharing Act of 2015, March 7, 2022, (Document is CUI)

1. (U) This is the Defense Intelligence Agency (DIA) Chief Information Officer (CIO), Cyber and Security Division (C&S), Operation Branch Chief response to the DoD Inspector General Report, "Management Advisory on DoD's Compliance with Cybersecurity Information Sharing Act of 2015" (Project No. D2021-D000CU-0078.001).

a. (U) **DoD IG RECOMMENDATION 2.a:** Guidance for removing personal information or information that
identified an individual from cybersecurity threats.

b. ~~(FOUO)~~ **DIA CIO, C&S, Operation Branch Chief Response 2.a:** DIA CIO, C&S, Operation Branch Chief agree with the recommendation. To mitigate this recommendation, Defense Intelligence Agency Computer Network Defense Center (DCNDC) modified paragraph 3.10.3 (Report Dissemination), bullet #3 to directly mention the removal of US Persons PII, not just DIA personnel in their [redacted]
[redacted]

c. (U) **DoD IG RECOMMENDATION 2.b:** Procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.

d. ~~(FOUO)~~ **DIA CIO, C&S, Operation Branch Chief Response 2.b:** DIA CIO, C&S, Operation Branch Chief agree with the recommendation. To mitigate this recommendation, Defense Intelligence Agency Computer Network Defense Center (DCNDC) modified paragraph 3.10.3 (Report Dissemination), bullet #11 in their [redacted] to comply with DoD IG Recommendation 2.b.

e. (U) **DoD IG RECOMMENDATION 2.c:** Procedures for notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure.

f. ~~(FOUO)~~ **DIA CIO, C&S, Operation Branch Chief Response 2.c:** DIA CIO, C&S, Operation Branch Chief agree with the recommendation. To mitigate this recommendation, Defense Intelligence Agency Computer Network Defense Center (DCNDC) modified paragraph 3.10.3 (Report Dissemination), bullet #12 in their [redacted] to comply with DoD IG Recommendation 2.c.

~~Classification: UNCLASSIFIED//FOUO~~

Defense Intelligence Agency (cont'd)

~~Classification: UNCLASSIFIED//FOUO~~

[redacted] March 28, 2022

2. (U) The point of contact for this matter is [redacted].

TORCH.CALLEEN.R.[redacted] Digitally signed by TORCH.CALLEEN.R[redacted] Date: 2022.04.13 12:33:18 -04'00'

Callen R. Torch
[redacted] DIA, CIO4C
Cyber Network Defense Branch Chief

1 Enclosure:

1. ~~(FOUO)~~ [redacted], February 23, 2022, ~~(Document is Unclassified//For Official Use Only)~~

~~Classification: UNCLASSIFIED//FOUO~~

Defense Counterintelligence and Security Agency

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY
27130 TELEGRAPH ROAD
QUANTICO, VA 22134-2253

MEMORANDUM FOR INSPECTOR GENERAL DEPARTMENT OF DEFENSE

SUBJECT: Management Advisory on DoD's Compliance With Cybersecurity Information Sharing Act of 2015 (Project No. D2021-D000CU-0078.001)

DCSA's "Enterprise Incident Response Plan Standard Operating Procedure," July 20, 2020, did not include guidance for removing personal information from CTIs; notifying individuals if personal information was shared in a CTI or defensive measure; or notifying Federal agencies that they received CTIs with known errors.

Recommendation 4

We recommend that the Defense Counterintelligence and Security Agency Chief Information Security Officer update and reissue the "Enterprise Incident Response Plan Standard Operating Procedure," July 20, 2020, ensuring it includes:

a. Guidance for removing personal information or information that identified an individual from cybersecurity threats.
b. Procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors, from other Federal agencies.
c. Procedures for notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure.

DCSA Response

DCSA will include language in the DCSA Enterprise Incident Response Plan:

a. Cyber (CCRM/CDO) will add language to the next version of the Enterprise Incident Response Plan Standard Operating Procedures that provides guidance for removing personal information or information that identified an individual from cybersecurity threats by 1 July 2022.
b. Cyber (CCRM/CDO) will add language to the next version of the Enterprise Incident Response Plan Standard Operating Procedures that provides guidance for notifying Federal agencies when we receive cyber threat indicators, containing known errors, from other Federal agencies by 1 July 2022.
c. Cyber (CCRM/CDO) will add language to the next version of the Enterprise Incident Response Plan Standard Operating Procedures that provides guidancefor notifying individuals that their personal information was shared as part of a cyber threat indicator or defensive measure by 1 July 2022.

LANDREAUX.ROXANNE.ACEVEDO.[redacted] Digitally signed by LANDREAUX.ROXANNE.ACEVEDO.[redacted] 12 09:43:13 -04'00'

Roxanne Landreaux
Authorizing Official
Defense Counterintelligence and Security Agency

National Geospatial-Intelligence Agency

UNCLASSIFIED

NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
7500 GEOINT Drive
Springfield, Virginia 22150

25 April 2022

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) DoD Response to Inspector General (IG), "Management Advisory on DoD's Compliance with Cybersecurity Information Sharing Act of 2015 (Project No. D2021-D000CU-0078.001) Draft Report.

(U) This is the National Geospatial-Intelligence Agency (NGA) Director of Cybersecurity Operations Center (CSOC), response to the DoD Inspector General draft report, "Management Advisory on DoD's Compliance with Cybersecurity Information Sharing Act of 2015," March 7, 2022 (Project No. D2021-D000CU-0078.001)

(U) **DoD IG RECOMMENDATION** 5: We recommend that the Director, Cybersecurity Operations Center, National Geospatial-Intelligence Agency, update and reissue the "Cyber Threat Intelligence Program Standards Operating Procedures" January 22,2021, ensuring it includes procedures for notifying Federal agencies that they received cyber threat indicators, containing known errors from other Federal agencies.

(U) **NGA Director of CSOC RESPONSE** 5: We agreed with the recommendation. We will update and reissue the "Cyber Threat Intelligence Program Standard Operating Procedures" in accordance with the DoD IG's recommendation.

(U) The point of contact for this matter is [redacted]

WHEELER.WESLEY.E.[redacted] Digitally signed by WHEELER.WESLEY.E.[redacted] Date: 2022.04.25 12:24:07 -05'00'

Wesley E. Wheeler
Director of Cybersecurity Operations Center

1

UNCLASSIFIED

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, 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
DoD Hotline 1.800.424.9098