Report No. DODIG-2021-100

~~SECRET//REL TO USA, FVEY~~

INSPECTOR GENERAL

U.S. Department of Defense

JULY 9, 2021

(U) Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations

Classified By: Carol N. Gorman
Derived From: Multiple Sources
Declassify On: 20450131

~~This content is classified at the SECRET//REL TO USA, FVEY level and contains elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to the applicable classification guide(s). It must be reviewed for both Classified National Security Information (CNSI) and CUI in accordance with DoDI 5230.09 prior to public release.~~

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

~~SECRET//REL TO USA, FVEY~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

(U) Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations

July 9, 2021

Objective

(U) The objective of this audit was to determine whether the DoD planned and executed activities to implement the memorandums between the DoD and the Department of Homeland Security (DHS) regarding cybersecurity and cyberspace operations. We conducted this audit in coordination with the DHS Office of Inspector General, which conducted a concurrent audit on the DHS activities taken to implement the memorandums. The DHS Office of Inspector General expects to issue a final report in FY 2021 with findings and recommendations specific to the DHS.

Background

(U) Since September 2010, the DoD and DHS have signed three interdepartmental memorandums to define the terms by which the DoD and DHS will collaborate to respond to and deter cyber threats to the United States and its critical infrastructure.

- (U) On September 27, 2010, the Secretaries of Defense and Homeland Security signed a memorandum to improve the coordination of each department's respective efforts regarding U.S. cybersecurity.
- (U) On November 25, 2015, the DHS Deputy Under Secretary for Cybersecurity and Communications, National Security Agency (NSA) Deputy Director, and U.S. Cyber Command (USCYBERCOM) Deputy Commander signed a memorandum to develop and maintain a cyber action plan to implement requirements outlined in the 2010 memorandum.
- (U) On October 6, 2018, the Secretaries of Defense and Homeland Security signed a memorandum to clarify the roles and responsibilities between the DoD and DHS for enhancing the U.S. Government's readiness to respond to cyber threats.

Findings

(U) DoD officials planned and executed activities to implement the 2010 and 2015 memorandums between the DoD and the DHS regarding cybersecurity and cyberspace operations. Examples of activities planned and executed in accordance with the 2010 and 2015 memorandums include the following.

- (U) The NSA and USCYBERCOM worked with the DHS to develop the cyber action plan, which contained goals, objectives, roles and responsibilities, and action items.
- (U) The NSA formalized the process used to exchange cyber indicators from the cyber indications and warnings process between the NSA, USCYBERCOM, and the DHS.
- ~~(U//FOUO)~~ [redacted]
- (U) USCYBERCOM developed a process for the DHS to request the DoD's assistance to support domestic cybersecurity preparedness and incident response.
- (U) The NSA and USCYBERCOM participated in cyber exercises and provided input for after action reports with the DHS.

(U) DoD officials also executed some activities to implement the 2018 memorandum, such as developing policy memorandums and participating in interagency meetings with DHS officials. However, the Cyber Protection and Defense Steering Group (CPD SG) has not developed an implementation plan with milestones and completion deadlines to ensure all activities to implement the 2018 memorandum are executed.

Results in Brief

(U) Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations

(U) Finding (cont'd)

(U) The co-chairs of the CPD SG stated that they did not develop an implementation plan because they did not intend for the 2018 memorandum to serve as a contractual agreement. Instead, the DoD CPD SG co-chairs stated the 2018 memorandum was developed to promote engagement between the DoD and DHS and define common areas of interest for collaboration.

(U) Without an implementation plan that clearly defines roles and responsibilities and identifies milestones and completion dates, the DoD may not be able to sustain collaboration with the DHS in protecting the Nation's critical infrastructure. Specific to the 2018 memorandum, the lack of an implementation plan could result in DoD officials not providing the level of assistance to the DHS needed for the DoD and the DHS to conduct joint operations to protect critical infrastructure; support state, local, tribal, and territorial governments; and jointly defend military and civilian networks from cyber threats. As stated previously, the DoD CPD SG co-chairs developed the 2018 memorandum to promote engagement between the DoD and the DHS and do not regard an implementation plan as necessary. However, if differences arise between the CPD SG co-chairs or as the membership changes, the lack of an implementation plan could hinder the level or timeliness of assistance requested and provided. In 2020, multiple Federal agencies and the private sector were compromised by malicious actors using a trusted source, SolarWinds Orion. Although the SolarWinds Orion compromise was not related to the lack of an implementation plan, the compromise continues to show the importance and criticality of the DoD's and DHS's ability to respond to any and all cyber threats, which would be significantly improved by implementing a plan to accomplish shared goals in the 2018 joint memorandum.

Recommendations

(U) We recommend that the Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff direct the DoD co-chairs of the Joint DoD-DHS CPD SG to work with the DHS co-chair to:

- (U) develop and approve plans of action and milestones for each line of effort; and
- (U) track activities executed and identify gaps that limit the DoD and DHS in fully implementing all lines of effort in the 2018 memorandum.

Management Comments

(U) The Deputy Secretary of Defense agreed with the recommendations to develop plans of action and milestones for the 2018 memorandum's lines of effort and track all collaborative activities related to protecting and defending critical infrastructure, gaps identified, and areas requiring improvements. The Vice Director of the Joint Staff, responding for the Chairman of the Joint Chiefs of Staff, disagreed with the recommendation to develop plans of action and milestones for the 2018 memorandum's lines of effort and did not address the specifics of the other recommendation to track activities and identify gaps in fully implementing the 2018 memorandum. However, the Vice Director stated that the Joint Staff planned to convene the CPD SG and achieve interdepartmental consensus on the best way to address the DoD Office of Inspector General's concerns. Therefore, we consider the planned actions by the Deputy Secretary of Defense and the Joint Staff sufficient to resolve the recommendations. We will close the recommendations once we verify that the action is complete.

(U) Please see the Recommendations Table on the next page for the status of recommendations.

(U)Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Deputy Secretary of Defense		1.a, 1.b	
Chairman of the Joint Chiefs of Staff		1.a, 1.b	**(U)**

(U) **NOTE**: The following categories are used to describe agency management's comments to individual recommendations.

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

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

July 9, 2021

(U) MEMORANDUM FOR DEPUTY SECRETARY OF DEFENSE
CHAIRMAN OF THE JOINT CHIEFS OF STAFF

(U) SUBJECT: Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations (Report No. DODIG-2021-100)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. Those comments are included in the report.

(U) This report contains two recommendations that we consider resolved and open. As described in the Recommendations, Management Comments, and Our Response section of this report, we will close the recommendations when you provide us documentation showing that all agreed-upon actions to implement the recommendations are completed. Therefore, please provide us within 90 days your response concerning specific actions in process or completed on the recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

(U) We appreciate the cooperation and assistance received during the audit. Please direct questions to me at [redacted].

Carol N. Gorman
Assistant Inspector General for
Audit Cyberspace Operations

Contents

(U) Introduction

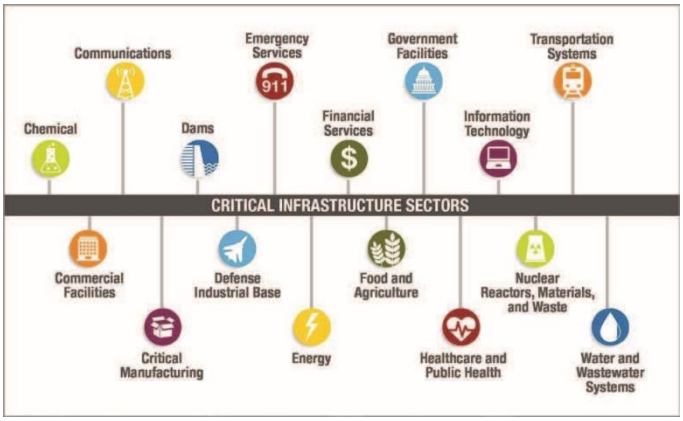
(U) Objective

(U) The objective of this audit was to determine whether the DoD planned and executed activities to implement the memorandums between the DoD and the Department of Homeland Security (DHS) regarding cybersecurity and cyberspace operations.
We conducted this audit in coordination with the DHS Office of Inspector General, which conducted a concurrent audit on the DHS activities taken to implement the memorandums. The DHS Office of Inspector General expects to issue a final report in FY 2021 with findings and recommendations specific to the DHS. See Appendix A for a discussion of the scope and methodology.

(U) Background

(U) Since September 2010, the DoD and the DHS have signed three interdepartmental memorandums to define the terms by which the DoD and the DHS will collaborate to respond to and deter cyber threats to the United States and its critical infrastructure. Critical infrastructure includes systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those. Examples of critical infrastructure in the United States include power, water, transportation, and communication systems.
The figure below identifies the 16 U.S. critical infrastructure sectors.

(U) Figure. 16 Critical Infrastructure Sectors in the United States



(U) Source: The DHS.

(U) Presidential Directives on Cybersecurity and Protecting Critical Infrastructure

(U) In December 2003, the President issued Homeland Security Presidential Directive (HSPD) 7, which established a national policy for Federal departments and agencies to identify and prioritize U.S. critical infrastructure and to protect it from terrorist attacks.[1] The Directive required the heads of all Federal departments and agencies to coordinate and cooperate with the Secretary of Homeland Security to protect critical infrastructure. HSPD-7 also required the Secretary of Homeland Security to maintain an organization that would work with Federal departments and agencies with cyber expertise to facilitate information sharing, vulnerability reduction and mitigation, and aid for national recovery efforts for critical infrastructure information systems.

(U) In January 2008, the President issued HSPD-23, which establishes U.S. policy, strategy, guidelines, and implementation actions to secure cyberspace.[2] HSPD-23 requires the U.S. Government to integrate many of its technical and organizational capabilities to better address sophisticated cybersecurity threats and vulnerabilities. The Directive states that the Secretary of Homeland Security will lead the effort to protect, defend, and reduce vulnerabilities of Federal systems and that the Secretary of Defense will provide support to the Secretary of Homeland Security with respect to the effort. HSPD-23 requires the Secretary of Homeland Defense to establish a National Cybersecurity Center to coordinate and integrate information to secure U.S. cyber networks and systems. The DoD is required to have representation at the National Cybersecurity Center. HSPD-23 also requires that each Federal agency that operates national security systems share information about security incidents, threats, and vulnerabilities to the extent consistent with standards and guidelines.[3]

[1] (U) Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003.

[2] (U) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008.

[3] (U) National security systems are any information system used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(U) In February 2013, the President issued Presidential Policy Directive (PPD) 21, which revoked HSPD-7, while authorizing any plans developed under HSPD-7 to remain in effect until revoked or superseded.[4] PPD-21 states that it is the policy of the United States to strengthen the security and resilience of its critical infrastructure against physical and cyber threats. Therefore, the U.S. Government will initiate efforts to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery actions related to critical infrastructure. The Directive requires agencies within the U.S. Government to work together to meet three strategic initiatives—(1) strengthen critical infrastructure security and resilience; (2) enable effective information exchange across the government; and (3) implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure. Specific to the DoD, PPD-21 requires the DoD to participate in the National Cyber Investigative Joint Task Force, which is headed by the Federal Bureau of Investigation and coordinates, integrates, and shares information related to cyber threat investigations.

(U) DoD and DHS Interdepartmental Memorandums

(U) The DoD and the DHS have issued three interdepartmental memorandums that address requirements in HSPD-7, HSPD-23, and PPD-21. The overall intent of the memorandums was to increase interdepartmental collaboration in strategic planning for national cybersecurity, mutual support for the development of cybersecurity capabilities, and coordination of operational cybersecurity mission activities, and to develop a cyber action plan and clarify each department's roles and responsibilities.

(U) September 2010 Memorandum

(U) In September 2010, the Secretaries of Defense and Homeland Security signed a memorandum to improve the coordination of each department's respective efforts regarding U.S. cybersecurity.[5] The 2010 memorandum established terms by which the DoD and the DHS would provide personnel, equipment, and facilities to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity. For example, under the memorandum, the DoD agreed to provide personnel to work with its DHS counterparts in support of the National Cybersecurity and Communications Integration Center, whose mission is to reduce the risk of systemic cybersecurity and communications challenges through cyber defense and incident response.

[4] (U) Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience," February 12, 2013.

[5] (U) "Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity," September 27, 2010.

(U) November 2015 Memorandum

(U) In November 2015, the DHS Deputy Under Secretary for Cybersecurity and Communications, National Security Agency (NSA) Deputy Director, and U.S. Cyber Command (USCYBERCOM) Deputy Commander signed a memorandum to develop and maintain a cyber action plan to implement requirements outlined in the 2010 memorandum.[6] Specifically, NSA and USCYBERCOM officials agreed to three overarching cybersecurity goals to increase:

- (U) the level of protection and defense of U.S. critical infrastructure;
- (U) U.S. Government cybersecurity and shared situational awareness; and
- (U) interagency coordination to enhance the prevention and mitigation of, response to, and recovery from domestic cybersecurity incidents.

(U) An Appendix to the 2015 memorandum contains the initial cyber action plan, which includes goals, objectives, action items, and the organizations responsible for leading and supporting each action item. The 2015 memorandum states that the DHS, the NSA, and USCYBERCOM agree to establish and charter a governance structure to oversee the routine management and activities of the cyber action plan. The NSA and USCYBERCOM are responsible for leading or jointly leading 21 of the action items in the cyber action plan. See Appendix B for a list of all 21 NSA- and USCYBERCOM-led action items in the 2015 memorandum. In addition, the DHS is responsible for leading or jointly leading 21 of the action items in the cyber action plan.

(U) October 2018 Memorandum

(U) In October 2018, the Secretaries of Defense and Homeland Security signed a memorandum to clarify the roles and responsibilities between the DoD and the DHS for enhancing the U.S. Government's readiness to respond to cyber threats.[7] The 2018 memorandum states that the DoD is responsible for supporting efforts to protect Defense Critical Infrastructure and Defense Industrial Base networks and systems from malicious cyber activity that could undermine U.S. military strength. The memorandum establishes six lines of effort (LOEs) to secure, protect, and defend the United States with a focus on cooperation and collaboration between the DoD and the DHS, as described in Table 1.

[6] (U) "Memorandum of Understanding Between Department of Homeland Security National Protection and Programs Directorate, National Security Agency, and United States Cyber Command for Implementation of the Cyber Action Plan," November 25, 2015.

[7] (U) "Joint Department of Defense-Department of Homeland Security Memorandum on Critical Infrastructure Defense/Protection Collaboration," October 6, 2018.

(U) Table 1. 2018 Memorandum Lines of Effort

(U) Line of Effort	Description
1. Intelligence, Indicators, and Warning	Improve protection and defense of critical infrastructure by enhancing DoD-DHS information sharing.
2. Strengthening the Resilience of National Critical Functions	Collaborate to improve the resilience of civilian-owned critical infrastructure that is critical to military operations and readiness.
3. Increasing the Joint Operational Planning and Coordination	Increase interoperability by jointly planning for and exercising incident response scenarios.
4. Incident Response	Conduct joint exercises to improve readiness ahead of a catastrophic cyber incident of national scale.
5. Integrating With State, Local, Tribal, and Territorial Governments	Collaborate to identify how the DoD may support the DHS's effort to secure and protect critical infrastructure owned or operated by state, local, tribal, and territorial governments.
6. Defense of Federal Networks	Coordinate efforts to defend military and civilian networks from cyber threats by sharing actionable and timely information. **(U)**

(U) Source: 2018 Memorandum.

(U) The 2018 memorandum states that the DoD and the DHS will establish a Joint DoD-DHS Cyber Protection and Defense Steering Group (CPD SG) to provide oversight for implementing the 2018 memorandum. The group's oversight responsibilities include approving a charter, identifying priority LOEs, and developing and overseeing an implementation plan with milestones and completion deadlines.

(U) DoD Action Items and Lines of Effort Reviewed

(U) Of the 21 action items in the 2015 memorandum that the NSA and USCYBERCOM are responsible for leading or jointly leading, we selected a nonstatistical sample of 13 of them to review. We also reviewed DoD actions taken to implement the six LOEs in the 2018 memorandum.

(U) Review of Internal Controls

(U) 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.[8] We identified internal control weaknesses in the DoD's oversight and governance over the implementation of the 2018 memorandum. We will provide a copy of the report to the Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff.

[8] (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

(U) Finding

(U) DoD Officials Planned and Executed Activities to Implement the 2010 and 2015 Memorandums but Have Not Developed an Implementation Plan for the 2018 Memorandum

(U) DoD officials planned and executed activities to implement the 2010 and 2015 memorandums between the DoD and the DHS regarding cybersecurity and cyberspace operations. Examples of activities planned and executed in accordance with the 2010 and 2015 memorandums include the following.

- (U) NSA and USCYBERCOM officials worked with DHS officials to develop the cyber action plan, which contained goals, objectives, roles and responsibilities, and action items.
- (U) NSA officials formalized the process used to exchange cyber indicators from the cyber indications and warnings process between the NSA, USCYBERCOM, and the DHS.
- ~~(U//FOUO)~~ [redacted]
- (U) USCYBERCOM officials developed a process for the DHS to request assistance for the DoD support of domestic cybersecurity preparedness and incident response.
- (U) NSA and USCYBERCOM personnel participated in cyber exercises and provided input for after action reports (AARs) with the DHS.

(U) DoD officials also executed some activities to implement the LOEs in the 2018 memorandum, such as developing policy memorandums and participating in interagency meetings with DHS officials. However, the CPD SG has not developed an implementation plan with milestones and completion deadlines to ensure all activities to implement the LOEs are executed.

(U) The co-chairs of the CPD SG stated that they did not develop an implementation plan because they did not intend for the 2018 memorandum to serve as a contractual agreement. Instead, the DoD CPD SG co-chairs stated the 2018 memorandum was

(U) developed to promote engagement between the DoD and DHS and define areas of common interest for collaboration. This occurred despite the CPD SG–approved CPD SG charter, which states that the co-chairs will approve plans of action and milestones for each LOE.

(U) Without an implementation plan that clearly defines roles and responsibilities and identifies milestones and completion dates, the DoD may not be able to sustain collaboration with the DHS in protecting the Nation's critical infrastructure. Specific to the 2018 memorandum, the lack of an implementation plan could result in DoD officials not providing the level of assistance to the DHS needed for the DoD and the DHS to conduct joint operations to protect critical infrastructure; support state, local, tribal, and territorial governments; and jointly defend military and civilian networks from cyber threats. As stated previously, the DoD CPD SG co-chairs developed the 2018 memorandum to promote engagement between the DoD and the DHS and do not regard an implementation plan as necessary. However, if differences arise between the CPD SG co-chairs or as the membership changes, the lack of an implementation plan could hinder the level or timeliness of assistance requested and provided. In 2020, multiple Federal agencies and the private sector were compromised by malicious actors using a trusted source, SolarWinds Orion. Although the SolarWinds Orion compromise was not related to the lack of an implementation plan, the compromise continues to show the importance and criticality of the DoD's and DHS's ability to respond to any and all cyber threats, which would be significantly improved by implementing a plan to accomplish shared goals in the 2018 joint memorandum.

(U) DoD Officials Planned and Executed Activities to Implement the 2010 and 2015 Memorandums

(U) DoD officials planned and executed activities to implement the 2010 and 2015 memorandums between the DoD and the DHS regarding cybersecurity and cyberspace operations. Examples of activities planned and executed in accordance with the 2010 and 2015 memorandums include the following.

- (U) NSA and USCYBERCOM officials worked with DHS officials to develop the cyber action plan, which contained goals, objectives, roles and responsibilities, and action items.

- (U) NSA officials formalized the process used to exchange cyber indicators from the cyber indications and warnings process between the NSA, USCYBERCOM, and the DHS.

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

- (U) USCYBERCOM officials developed a process for the DHS to request DoD support of domestic cybersecurity preparedness and incident response.

- (U) NSA and USCYBERCOM personnel participated in cyber exercises and provided input for AARs with the DHS.

(U) The NSA and USCYBERCOM officials executed agreed-upon activities to implement the action items in the 2015 memorandum.

(U) DoD Officials Developed a Cyber Action Plan

(U) To achieve the three goals in the 2015 memorandum, NSA, USCYBERCOM, and DHS officials developed a cyber action plan, which established 13 objectives and 32 action items. For example, to increase the level of protection and defense of U.S. critical infrastructure, NSA, USCYBERCOM, and DHS officials developed an objective to formalize the process by which NSA, USCYBERCOM, and DHS officials exchange cyber indicators from the cyber indications and warning process. NSA, USCYBERCOM, and DHS officials developed three action items to meet this objective, which included the NSA leading efforts to establish and document a formal process that defines information requirements, identifies exchange parameters, and enables a recurring review to ensure relevance and validity.

(U) To increase interagency coordination and enhance the prevention and mitigation of, response to, and recovery from domestic cybersecurity incidents, NSA, USCYBERCOM, and DHS officials developed an objective to perform interagency training and exercises to increase shared awareness of operational capabilities and to enhance coordination, mitigation, and response to cybersecurity incidents. NSA, USCYBERCOM, and DHS officials developed five action items to meet this objective, which included USCYBERCOM leading efforts to coordinate with the Office of the Under Secretary of Defense for Policy (OUSD[P]) and Joint Staff to determine a concept of operations of USCYBERCOM Cyber Protection Teams when employed off the DoD information networks during a domestic cybersecurity event. Furthermore, the NSA, USCYBERCOM, and the DHS were responsible for leading three of the five action items, including conducting cooperative training activities, mission rehearsals, and other information exchanges to increase shared understanding of roles and responsibilities and operational capabilities.

(U) The NSA Formalized Information Exchange Processes Between the NSA, USCYBERCOM, and the DHS

(U) NSA officials formalized the process that NSA, USCYBERCOM, and DHS officials use to exchange cyber indicators from the cyber indications and warnings process. Specifically, NSA officials established a process that defines information requirements,

(U) identifies exchange parameters, and allows for the review of cyber indicators. In addition, NSA officials used various tools to facilitate the exchange of classified and unclassified cyber threat indicators.

(U) According to the 2015 memorandum, to enable proactive planning and response to cyber indicators, the NSA Deputy Director agreed that the NSA would lead the establishment of a process that defines information requirements, identifies exchange parameters, and enables recurring reviews of information for relevance and validity. In addition, the NSA Deputy Director agreed that the NSA would lead the identification, development, and use of mutually beneficial tools to facilitate cyber information exchange. To determine whether NSA officials developed a process and used tools for cyber information exchange, we reviewed policy documents and the NSA information exchange process flowchart. In addition, we visited the Integrated Cyber Center operations floor to observe how the NSA shares indicators with the DHS.[9]

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

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

[9] (U) The Integrated Cyber Center is located at Fort Meade, Maryland.

[10] (U) NSA Central Security Service Policy 11-1, "Information Sharing" March 28, 2012. Signals intelligence is information important to national or homeland security that is derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.

[11] (U) NSA Central Security Service Policy 11-11, "National Security Agency Central Security Service Cybersecurity Signatures and Indicators of Malicious Cyber Activity," March 26, 2019. Signatures are text strings used to configure intrusion detection systems and sensors. Signatures describe the characteristics, patterns, or other identifying information about cyber threat activity. Indicators are patterns of relevant, observable adversary activity in a given operational cyber domain.

[12] (U) The flowchart we received is called the "Current Indicator/Signature Sharing Workflow." This is a living document we received on January 7, 2020. We received a narrative for the flowchart entitled "NSA's Process to Proactively Share Cyber Threat Indicators with the DHS." This narrative is a living document that we received on January 7, 2020.

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

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

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

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

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

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

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

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

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

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

(U) USCYBERCOM Developed a Process for the DHS to Request Assistance from the DoD and USCYBERCOM

(U) USCYBERCOM officials developed a process for the DHS to request assistance for the DoD support of domestic cybersecurity preparedness and incident response. According to the 2015 memorandum, the USCYBERCOM Deputy Commander agreed to coordinate with the OUSD(P) and Joint Staff to develop recommendations to determine and refine formal processes for the DHS to request assistance, as appropriate, for DoD or USCYBERCOM support across all phases of domestic cybersecurity preparedness and incident response. To determine whether USCYBERCOM developed a process for the DHS to request DoD assistance, we reviewed DoD policies and interviewed USCYBERCOM and DHS officials.

(U) USCYBERCOM officials stated that they follow DoD Directive 3025.18 and Directive-Type Memorandum 17-007 when receiving and responding to DHS requests for assistance.[17] DoD Directive 3025.18 establishes policy and assigns responsibility for Defense Support of Civil Authorities and provides guidance for the execution and oversight of Defense Support for Civil Authorities when requested by qualifying entities and approved by DoD officials.[18] Specifically, DoD Directive 3025.18 states that all requests for Defense Support for Civil Authorities must be written and include a commitment to reimburse the DoD and be submitted to the Office of the Executive

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

[16] (U) The Cybersecurity and Infrastructure Security Agency is a DHS Component.

[17] (U) DoD Directive 3025.18, "Defense Support of Civil Authorities," December 29, 2010 (incorporating Change 2, March 19, 2018). Directive-Type Memorandum 17-007, "Interim Policy and Guidance for Defense Support to Cyber Incident Response," June 21, 2017 (incorporating Change 2, June 6, 2019).

[18] (U) Defense Support for Civil Authorities is support provided by U.S. Federal military forces, DoD civilians, DoD contract personnel, DoD Component assets, and National Guard forces in response to requests for assistance from civil authorities for domestic emergencies, law enforcement support, and other domestic activities, or from qualifying entities for special events.

(U) Secretary of the DoD. DoD Directive 3025.18 also states that during an emergency, oral requests for assistance must be followed by a written request that includes an offer to reimburse the DoD at the earliest opportunity. Directive-Type Memorandum 17-007 provides policy guidance, assigns responsibilities, and details procedures for providing Defense Support to Cyber Incident Response. Specifically, Directive-Type Memorandum 17-007 states that requests for Defense Support to Cyber Incident Response will be evaluated with the criteria established in DoD Directive 3025.18. According to DHS officials, the DHS also uses other means to request DoD assistance, such as Section 1650 of the National Defense Authorization Act for FY 2019, which allows the DoD to send up to 50 DoD personnel to the DHS to enhance cybersecurity cooperation, collaboration, and unity of Government efforts.[19]

(U) The NSA and USCYBERCOM Participated in Cyber Exercises and Provided Input for After Action Reports

(U) NSA and USCYBERCOM officials participated in cyber exercises, provided input for AARs, and established a process for integrating findings and recommendations identified in AARs.[20] According to the 2015 memorandum, the NSA Deputy Director and USCYBERCOM Deputy Commander agreed to ensure proper representation and participation in cyber exercise AARs and establish formal mechanisms for integrating findings and recommendations into management processes for resolution. Interagency exercises include joint training designed to prepare national-level organizations and combatant commanders and staff at the strategic and operational levels of war to integrate interagency, non-governmental, and multinational partners in highly complex environments. To determine whether NSA and USCYBERCOM officials participated in cyber exercise AARs and established a process for integrating findings and recommendations, we reviewed AARs for interagency cyber exercises conducted from November 2015 to November 2017 and USCYBERCOM guidance regarding USCYBERCOM's lessons learned program.[21] In addition, we interviewed NSA and USCYBERCOM officials.

(U) NSA, USCYBERCOM, and DHS officials participated in two joint cyber exercises from November 2015 to November 2017, CYBER GUARD 16 and CYBER GUARD 17. CYBER GUARD is an annual exercise co-led by USCYBERCOM, the DHS, and the Federal Bureau of Investigation designed to support a wide range of military tests and exercises, which includes response to destructive cyber attacks against U.S. critical infrastructure.

[19] (U) Public Law 115-232, "John S. McCain National Defense Authorization Act for Fiscal Year 2019," section 1650, "Pilot Program Authority to Enhance Cybersecurity and Resiliency of Critical Infrastructure," August 13, 2018.

[20] (U) An AAR is a summary report that identifies key observations of deficiencies and strengths, and focuses on performance of specific mission-essential tasks.

[21] (U) We reviewed cyber exercises conducted from November 2015 through November 2017. There were only two joint large-scale cyber exercises conducted during this timeframe.

(U) USCYBERCOM officials stated that after each exercise, each organization that participated in the exercise provides at least one representative to participate in the AAR. According to the AARs for CYBER GUARD 16 and CYBER GUARD 17, NSA and USCYBERCOM officials participated in the AARs.

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

(U) USCYBERCOM Instruction 1200-05 establishes policy and provides guidance for implementing the Joint Lessons Learned Program, as outlined in Chairman of the Joint Chiefs of Staff guidance.[22] According to Chairman of the Joint Chiefs of Staff Manual 3150.25B, the Joint Lessons Learned Program exists to capture and process observations; leverage change mechanisms; and institutionalize and disseminate lessons learned to improve readiness, capabilities, and combat performance.[23] USCYBERCOM Instruction 1200-05 further establishes procedures for identifying, tracking, and resolving observations and issues affecting exercises and training events hosted and supported by USCYBERCOM.

~~(CUI)~~ The AARs for CYBER GUARD 16 and CYBER GUARD 17 included findings, recommendations, and the status of each recommendation. [redacted]

[22] (U) USCYBERCOM Instruction 1200-05, "Joint Lessons Learned Program," February 20, 2020.

[23] (U) Chairman of the Joint Chiefs of Staff Manual 3150.25B, "Joint Lessons Learned Program," October 12, 2018.

(U) DoD Officials Executed Some Activities to Implement the 2018 Memorandum, but An Implementation Plan is Needed

(U) Although the CPD SG co-chairs did not develop an implementation plan with milestones and completion dates, DoD officials executed some activities to implement the LOEs in the 2018 memorandum. For example, DoD officials developed policy memorandums and participated in interagency meetings with DHS officials. Table 2 summarizes the activities that the DoD executed or that OUSD(P) officials stated that the DoD executed to implement the LOEs.

(U) Table 2. DoD Activities Related to Lines of Effort in 2018 Memorandum

(U) Lines of Effort		Related Activities
1. Intelligence, Indicators, and Warnings	Enhance DoD-DHS information sharing.	Participate in relevant National Security Council/interagency meetings Develop Pathfinder Frameworks
	Improve information sharing between the Departments and the private sector.	Participate in relevant National Security Council/interagency meetings Develop Pathfinder Frameworks
	Improve mechanisms for timely sharing of actionable information.	Issue Exception to Policy Memorandum 16-002 Develop Pathfinder Frameworks
	Address gaps in intelligence collection and joint analysis.	Develop Pathfinder Frameworks
2. Strengthening the Resilience of National Critical Functions	Jointly work with interagency partners to establish programs and projects to ensure the continuity of military and civilian functions.	Participate in relevant National Security Council/interagency meetings Develop Pathfinder Frameworks
3. Increasing Joint Operational Planning and Coordination	Work with other Federal departments and agencies to develop and execute campaign plans.	Participate in relevant National Security Council/interagency meetings
	Jointly plan for and exercising incident response scenarios.	Develop plan of action and milestones in response to the FY 2018 National Defense Authorization Act Section 1649 Complete Table Top Exercise Report Executive Summary to meet Section 1649 requirements **(U)**

(U) Table 2. DoD Activities Related to Lines of Effort in 2018 Memorandum (cont'd)

(U) Lines of Effort		Related Activities
4. Incident Response	Establish agreements to expedite and enhance incident-response operations and improve information sharing.	Issue Exception to Policy Memorandum 16-002 Develop Pathfinder Frameworks
	Conduct joint exercises to improve readiness ahead of a catastrophic cyber incident of national scale.	Develop plan of action and milestones in response to the FY 2018 National Defense Authorization Act Section 1649
5. Integrating with State, Local, Tribal, and Territorial Governments	Clarify roles and responsibilities (including how states may use their National Guard personnel in state active duty).	Issue Exception to Policy Memorandum 16-002
	Identify how the DoD may support the DHS's efforts to secure and protect critical infrastructure owned or operated by state, local, tribal, and territorial governments.	Issue Policy Memorandum 16-002
6. Defense of Federal Networks	Share actionable and timely information.	Participate in relevant National Security Council/interagency meetings Develop Pathfinder Frameworks
	Explore developing information-sharing agreements with other U.S. departments and agencies and key allies.	Participate in relevant National Security Council/interagency meetings Develop Pathfinder Frameworks
	Establish agreements to expedite and enhance incident-response operations and improve information sharing.	Issue Policy Memorandum 16-002 **(U)**

(U) Source: The OUSD(P).

(U) We reviewed OUSD(P)-provided documentation associated with the related activities to determine whether DoD officials executed activities to implement the LOEs from the 2018 memorandum. In addition, we determined that some of the activities executed to implement the 2018 memorandum complement the action items implemented for the 2015 memorandum, such as information sharing between the DoD and DHS.

(U) Activities Executed for Integrating With State, Local, Tribal, and Territorial Governments

(U) DoD officials executed some activities for integrating with state, local, tribal, and territorial governments. The LOE states:

> (U) DoD and DHS will collaborate to identify how DoD may support DHS's efforts to secure and protect critical infrastructure owned or operated by state, local, tribal, and territorial governments. DoD will support DHS efforts to plan with state, local, tribal, and territorial governments to clarify roles and responsibilities (including how States may use their National Guard personnel in State active duty), and will conduct operations planning for supporting DHS activities in support of state, local, tribal, and territorial authorities. For example, given the unique challenges and sensitivity of protecting elections infrastructure, DoD and DHS will collaborate as they carry out their responsibilities, with DoD continuing to prioritize its mission to preempt, defeat, or deter malicious cyber activity targeting the United States, which will help counter significant threats to democratic institutions.

(U) OUSD(P) officials stated that Policy Memorandum 16-002 and Exception to Policy Memorandum 16-002 implemented this LOE.[24] Specifically, OUSD(P) officials stated that Policy Memorandum 16-002 identifies how the DoD may support the DHS's efforts to secure and protect critical infrastructure owned or operated by state, local, tribal, and territorial governments. Policy Memorandum 16-002 allows DoD Components to consult with government entities, public and private utilities, critical infrastructure owners, the Defense Industrial Base, and other non-governmental entities to:

- (U) protect DoD information networks, software, and hardware;
- (U) enhance DoD cyber situational awareness;
- (U) provide for DoD mission assurance requirements; and
- (U) provide cybersecurity unity of effort.

[24] (U) Transition of Policy Memorandum 16-002, "Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities," undated. Exception to Policy Memorandum 16-002, "Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DoD Information Networks, Software, and Hardware for State Cyberspace Activities," October 18, 2018.

(U) OUSD(P) officials stated that the Exception to Policy Memorandum 16-002 clarifies roles and responsibilities, including how states may use their National Guard personnel in state active duty. The Exception to Policy Memorandum 16-002 authorizes the National Guard access to classified national security information in support of elections security. In addition to issuing Exception to Policy Memorandum 16-002 to address elections security, DoD officials executed other activities to protect elections infrastructure during the 2018 and 2020 U.S. elections. Specifically, DoD officials:

- (U) approved a request for assistance memorandum submitted by the DHS for cyber incident response for the 2018 U.S. elections;
- (U) developed a concept of operations that identified elections security objectives and related DoD roles and responsibilities for the 2018 U.S. elections;
- (U) developed an AAR based on the DoD's execution of an operation supporting 2018 elections security;
- (U) jointly created a lessons learned document with the DHS that provided key observations, challenges, and recommendations related to the 2018 elections cycle; and
- ~~(S//REL TO USA, FVEY)~~ [redacted]

(U) However, Policy Memorandum 16-002 and Exception to Policy Memorandum 16-002 do not discuss how the DoD would support DHS efforts or clarify roles and responsibilities related to assisting DHS efforts to secure and protect critical infrastructure owned or operated by state, local, tribal, and territorial governments.

(U) Activities Executed for Strengthening the Resilience of National Critical Functions

(U) DoD officials executed some activities for strengthening the resilience of national critical functions. The LOE states:

> (U) DoD and DHS will collaborate to improve the resilience of civilian-owned critical infrastructure that is critical to military operations and readiness. DoD and DHS will jointly work with interagency partners to establish programs and projects to ensure the continuity of military and civilian essential functions to reduce consequences resulting from strategic cyber threats.

(U) OUSD(P) officials stated that developing the frameworks for the Pathfinder Initiatives and participating in National Security Council briefings and interagency meetings implemented this LOE.

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

(U) In addition, OUSD(P) officials stated that the OUSD(P) participates in monthly meetings with sub-policy coordination committees to discuss critical infrastructure cybersecurity roles and responsibilities and biweekly meetings with the Federal Senior Leadership Council Working Group to discuss cyber roles and responsibilities led by the DHS.[25] However, OUSD(P) officials did not provide minutes or agendas for the meetings.

(U) DoD Officials Have Not Developed an Implementation Plan for the 2018 Memorandum

(U) The CPD SG did not develop a plan to implement the 2018 memorandum to ensure all activities to implement the LOEs are executed. The 2018 memorandum states the DoD and DHS will establish a CPD SG to guide and oversee the implementation of the memorandum. The CPD SG is co-chaired by the Assistant Secretary of Defense for Homeland Defense and Global Security; the Assistant Secretary of Homeland Security for Cyber, Infrastructure, and Resilience Policy; the Joint Staff Director for Command, Control, Communications, and Computers (Cyber, J6); and the Assistant Secretary of Homeland Security for Cybersecurity and Communications. The 2018 memorandum

[25] (U) National Security Council policy coordination committees manage the development and implementation of national security policies by multiple U.S. Government agencies. Policy coordination committees support interagency coordination of national security policy; provide policy analysis for consideration by more senior committees of the National Security Council system; and ensure timely responses to decisions made by the President. The Federal Senior Leadership Council was established in the National Infrastructure Protection Plan to drive enhanced communications and coordination with respect to critical infrastructure security and resilience matters among Federal departments and agencies.

(U) states that within 30 days of the signing of the 2018 memorandum, the CPD SG will approve a charter and develop and oversee an implementation plan with milestones.

(U) In November 2018, the CPD SG approved the CPD SG charter, which states that the co-chairs will approve plans of action and milestones for each LOE. However, the CPD SG co-chairs did not develop plans of action and milestones for the LOEs. The co-chairs of the CPD SG stated that they did not develop an implementation plan because they did not intend for the 2018 memorandum to serve as a contractual agreement. Instead, the DoD CPD SG co-chairs stated the 2018 memorandum was developed to promote engagement between the DoD and the DHS and define areas of common interest for collaboration.

(U) In October 2005, the Government Accountability Office issued a report that identified key practices that can help enhance and sustain interagency collaboration.[26] The key practices include agreeing on roles and responsibilities and creating the means to monitor and evaluate efforts. The Government Accountability Office report states that collaborating agencies should work together to define and agree on their respective roles and responsibilities, including how the collaborative effort will be led. By agreeing on roles and responsibilities, agencies clarify joint and individual efforts and facilitate decision making. The CPD SG co-chairs did not define DoD and DHS roles and responsibilities for implementing the LOEs. For example, LOE No. 2 states that the DoD and the DHS will collaborate to improve the resilience of civilian-owned critical infrastructure that is critical to military operations and readiness. However, the CPD SG co-chairs did not identity roles and responsibilities for implementing the LOE.

(U) The Government Accountability Office report also states that Federal agencies engaged in collaboration need to create the means to monitor and evaluate their efforts in order to identify areas for improvements. Developing mechanisms to monitor, evaluate, and report results can help key decision makers within the agencies obtain the feedback needed to improve policy and operational effectiveness. According to the DHS CPD SG co-chair, there should be an oversight mechanism put in place to monitor progress of operational activities related to the 2018 memorandum.

(U) To organize DoD and DHS joint and individual efforts and facilitate decision making to address the threats the United States faces in cyberspace, the Deputy Secretary of Defense and Chairman of the Joint Chiefs of Staff should direct the DoD CPD SG co-chairs to work with the DHS CPD SG co-chair to develop and approve plans of action and milestones for each LOE. For example, the 2015 memorandum contained the initial cyber action plan, which included goals, objectives, action items, and the organizations

[26] (U) GAO-06-15, "Results-Oriented Government: Practices That Can Help Enhance and Sustain Collaboration Among Federal Agencies," October 2005.

(U) responsible for leading and supporting each action item. Furthermore, to provide key DoD decision makers feedback for improving policy and operational effectiveness related to implementing the LOEs, the Deputy Secretary of Defense and Chairman of the Joint Chiefs of Staff should direct the DoD CPD SG co-chairs to work with the DHS CPD SG co-chairs to track activities executed and identify gaps that limit the DoD and DHS in fully implementing all LOEs in the 2018 memorandum.

(U) The DoD May Not Be Able to Sustain Collaboration With the DHS in Protecting Critical Infrastructure

(U) Without an implementation plan that clearly defines roles and responsibilities and identifies milestones and completion dates, the DoD may not be able to sustain collaboration with the DHS in protecting the Nation's critical infrastructure. Specific to the 2018 memorandum, the lack of an implementation plan could result in DoD officials not providing the level of assistance to the DHS needed for the DoD and the DHS to conduct joint operations to protect critical infrastructure; support state, local, tribal, and territorial governments; and jointly defend military and civilian networks from cyber threats. As stated previously, the DoD CPD SG co-chairs developed the 2018 memorandum to promote engagement between the DoD and the DHS and do not regard an implementation plan as necessary. However, if differences arise between the CPD SG co-chairs or as the membership changes, the lack of an implementation plan could hinder the level or timeliness of assistance requested and provided. In 2020, multiple Federal agencies and the private sector were compromised by malicious actors using a trusted source, SolarWinds Orion. Although the SolarWinds Orion compromise was not related to the lack of an implementation plan, the compromise continues to show the importance and criticality of the DoD's and DHS's ability to respond to any and all cyber threats, which would be significantly improved by implementing a plan to accomplish shared goals in the 2018 joint memorandum.

(U) Recommendations, Management Comments, and Our Response

(U) RECOMMENDATION 1

(U) We recommend that the Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff direct the DoD co-chairs of the Joint DoD-Department of Homeland Security Cyber Protection and Defense Steering Group to work with the Department of Homeland Security co-chair of the Joint DoD-Department of Homeland Security Cyber Protection and Defense Steering Group to:

a. **(U) Develop and approve plans of action and milestones for each line of effort.**

(U) Deputy Secretary of Defense Comments

(U) The Deputy Secretary of Defense agreed with the recommendation, stating that the DoD would draft plans of action and milestones for the 2018 memorandum's LOEs when they did not duplicate incident response efforts or National Security Council-directed operational planning.

(U) Joint Staff Comments

(U) The Vice Director of the Joint Staff, responding for the Chairman of the Joint Chiefs of Staff, disagreed, stating that the Joint Staff did not support establishing new, broad plans of action and milestones for the six LOEs described in the 2018 memorandum. The Vice Director further stated that substantial cross-over exists with current National Cyber Strategy LOEs and existing plans of action and milestones. According to the Vice Director, establishing additional plans of action and milestones in a reactionary manner may result in confusion over roles and responsibilities, decrease economy of effort, and ultimately delay the tasks that the CPD SG was established to oversee. Furthermore, the Vice Director stated that the Joint Staff planned to convene the CPD SG and achieve interdepartmental consensus on the best way to address the DoD Office of Inspector General's concerns.

(U) Our Response

(U) Although the Vice Director of the Joint Staff disagreed with the recommendation, planned actions by the Deputy Secretary of Defense and the Joint Staff address all specifics of the recommendation. In March 2021, a Joint Staff official provided a DoD Cyber Strategy project plan that included milestones, lead offices, metrics, and outcomes for five of the six LOEs in the 2018 memorandum. Based on the Vice Director's plans to achieve interdepartmental consensus on the best way to address our concerns and the Deputy Secretary of Defense's plan to develop plans of action and milestones for the 2018 memorandum's LOEs when not duplicative, the

(U) recommendation is resolved but will remain open. We will close the recommendation once we verify that the plans of action and milestones, approved by the co-chairs of the CPD SG, address each LOE in the 2018 memorandum.

b. (U) Track activities executed and identify gaps that limit the DoD and the Department of Homeland Security in fully implementing all lines of effort in the 2018 memorandum.

(U) Deputy Secretary of Defense Comments

(U) The Deputy Secretary of Defense agreed with the recommendation, stating that the DoD would track all collaborative activities related to protecting and defending critical infrastructure, gaps identified, and areas requiring improvements.

(U) Joint Staff Comments

(U) The Vice Director of the Joint Staff, responding for the Chairman of the Joint Chiefs of Staff, did not agree or disagree with the recommendation. However, the Vice Director stated that the Joint Staff planned to convene the CPD SG and achieve interdepartmental consensus on the best way to address the DoD Office of Inspector General's concerns.

(U) Our Response

(U) Although the Vice Director of the Joint Staff did not agree or disagree with the recommendation, planned actions by the Deputy Secretary of Defense and the Joint Staff address all specifics of the recommendation. Therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the co-chairs of the CPD SG tracked activities executed and identified gaps that limit the DoD and DHS in fully implementing all LOEs in the 2018 memorandum.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this performance audit from July 2019 through December 2020; however, the audit was suspended from March 14, 2020, through October 15, 2020, due to the DoD's implementation of maximum telework during the coronavirus disease-2019 pandemic. We conducted this performance audit in accordance with generally accepted government auditing standards, which 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

(U) We reviewed three memorandums between the DoD and the DHS regarding cybersecurity and cyberspace operations signed in 2010, 2015, and 2018. We conducted this audit in coordination with the DHS Office of Inspector General, which conducted a concurrent audit on the DHS activities taken to implement the memorandums. The DHS Office of Inspector General expects to issue a final report in FY 2021 with findings and recommendations specific to the DHS.

(U) The 2015 memorandum included 13 objectives and 32 action items to achieve those objectives. According to the 2015 memorandum, the NSA and USCYBERCOM were responsible for leading 10 of the 32 action items. In addition, the NSA, USCYBERCOM, and DHS were responsible for jointly leading 11 of the 32 action items. We selected a nonstatistical sample of 13 of the 21 action items led by the NSA and USCYBERCOM for review that we determined were measurable.[1] See Appendix B for the list of objectives and action items. We interviewed officials from the NSA and USCYBERCOM to obtain an understanding of their actions to execute the 13 action items and reviewed documentation, such as USCYBERCOM and NSA cyber policies, information sharing processes, and cyber exercise AARs to validate the action taken.

(U) We interviewed OUSD(P) officials to determine how the DoD executed the six LOEs in the 2018 memorandum. In addition, we interviewed the CPD SG co-chairs to obtain an understanding of their roles and responsibilities related to oversight of the 2018 memorandum. In addition, we attended a CPD SG meeting to observe how the CPD SG implements the LOEs. Furthermore, we reviewed the Joint CPD SG Charter, the

[1] (U) We determined an action item to be measurable if the action item did not require the NSA or USCYBERCOM to: (1) identify or explore opportunities regarding a task, or (2) review a document. Of the 21 action items led by either the NSA or USCYBERCOM, we determined that 8 were not measurable.

(U) Joint CPD SG meeting minutes, and documentation provided by OUSD(P) officials that shows activities performed aligning with the LOEs.

(U) The primary audit locations were the Pentagon, Arlington, Virginia; DHS, Arlington, Virginia; and Fort Meade, Maryland.

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this audit.

(U) Prior Coverage

(U) No prior coverage has been conducted on the memorandums between the DoD and the DHS regarding cybersecurity and cyberspace operations during the last 5 years.

(U) Appendix B

(U) 2015 Cyber Action Plan Objectives and Action Items Led by the DoD

(U) The table below summarizes the 8 objectives and 21 associated action items led by the NSA and USCYBERCOM for each goal described in the 2015 memorandum.

(U) Objective	Action Item	DoD Component Lead
Goal: Increase the level of protection and defense of U.S. critical infrastructure.		
Formalize the process by which the DHS, the NSA, and USCYBERCOM exchange cyber indications and warnings information at an operational tempo that enables proactive planning and response.	Establish and document a formal process that defines information requirements, identifies exchange parameters (for example, classification levels), and enables a recurring review to ensure relevance and validity. *	NSA
	Identify, develop, and/or leverage existing mutual beneficial tools, such as CYBER COP, to facilitate cyber information exchange. *	NSA
	Perform follow-on actions to fully implement mutually beneficial cyber information exchange capabilities to include: exchange of technical representatives, adoption of emerging Enhanced Shared Situational Awareness capabilities, full integration of event/incident data across organizations, comprehensive access to screens and views consistent with authorities, and continued provision of training and support. *	NSA
Establish cross-organization analytic capabilities that enable analysts and operators to share results and support synchronized operational actions in accordance with access control and legal and compliance regulations.	Establish initial capabilities that share DHS, NSA, and USCYBERCOM data for other organizations' use in their "local" analytics. *	NSA
	Establish initial capabilities that enable "community" analytics to run across the DHS, NSA, and USCYBERCOM data sets and provide results using Information Sharing Architecture Structured Threat Information eXpression profiles. *	NSA
Goal: Increase U.S. government cybersecurity and shared situational awareness, by creating consistent approaches across both national security and non-national security systems. **(U)**		

(U) Objective	Action Item	DoD Component Lead
Evaluate the potential for implementing DHS's Continuous Diagnostics and Mitigation tools on national security systems.	Explore opportunities for National Security System organizations to leverage the General Services Administration blanket purchase agreement applicable tools and services along with the Continuous Diagnostics and Mitigation dashboard.	NSA
Ensure the consistent and appropriate functioning of the NSA Cryptologic Services Group support to the DHS.	Officially establish and resource the NSA Cryptologic Services Group at the DHS to ensure the capability to complete assigned tasks as defined by the DHS/National Protection and Programs Directorate and NSA/Central Security Service Memorandum of Agreement. *	NSA
Develop scalable operational capabilities and standards to support situational awareness and cyber-relevant action through the integration of commercial products, including the interagency Enterprise Automated Security Environment efforts, and offering customizable levels of semi-automated and automated decision making processes that can be used for national security system and non-national security system federal and private sector applications.	Develop technical concepts and roadmaps relating to Enterprise Automated Security Environment. *	NSA
	Work with the National Institute of Standards and Technology to identify opportunities in developing specific standards relating to the Enterprise Automated Security Environment.	NSA
	Develop a Joint Enterprise Automated Security Environment Reference Architecture and Reference Requirement Set to enable coordinated engagement with vendors and joint capability development. *	NSA
	Explore opportunities for joint research and technology assessment activities relating to Enterprise Automated Security Environment, leveraging the Department of Energy National Labs to create an enduring supply of cybersecurity ideas and researched prototypes.	NSA
	Explore opportunities for joint engagement with industry and academia relating to Enterprise Automated Security Environment and plan joint Enterprise Automated Security Environment-related pilots in accordance with all applicable laws, regulations, and policies.	NSA
Goal: Increase interagency coordination and operational integration to enhance prevention and mitigation of, response to, and recovery from domestic cybersecurity incidents. **(U)**		

(U) Objective	Action Item	DoD Component Lead
Perform interagency training and exercises to increase shared awareness of operational capabilities and to enhance coordination, mitigation, and response to cybersecurity incidents.	Identify and resolve resourcing, planning, and policy issues that inhibit full organizational participation as appropriate in large-scale cyber exercises, such as Cyber Guard, Cyber Storm, and National Level Exercises. *	NSA, USCYBERCOM
	Ensure proper representation and participation in cyber exercise AARs and establish forum mechanisms for integrating findings and recommendations into management processes for resolution. *	NSA, USCYBERCOM
	Conduct cooperative training activities, mission rehearsals, and other information exchanges to increase shared understanding of roles, responsibilities and operational capabilities, such as incident response teams. *	NSA, USCYBERCOM
	Coordinate with [OUSD(P)] and Joint Staff to determine concept of operations of USCYBERCOM Cyber Protection Teams when/if employed off the Department of Defense Information Networks during a domestic cybersecurity event. *	USCYBERCOM
Review, refine, and develop as required streamlined processes for formal requests for support or assistance between the DHS, the NSA, and USCYBERCOM.	Review the Request for Technical Assistance process when NSA capabilities would be provided during a national domestic cyber event.	NSA
	Coordinate with [OUSD(P)] and Joint Staff and develop recommendations to determine and refine formal processes for the DHS to request assistance, as appropriate, through the DoD for USCYBERCOM support across all phases of domestic cybersecurity preparedness and incident response. *	USCYBERCOM
Review, as required, applicable memorandums of agreement, memorandums of understanding, or other associated agreements between the DHS, the NSA, and USCYBERCOM and recommend changes or	Review the memorandum of agreement between the DHS and DoD regarding cybersecurity (signed September 2010).	NSA, USCYBERCOM
	Review the memorandum of agreement between the NSA Central Security Service and DHS National Protection and Programs directorate for the establishment and operation of a CSG.	NSA, USCYBERCOM **(U)**

(U) Objective	Action Item	DoD Component Lead
updates as appropriate to ensure current relevance in enhancing national cybersecurity efforts.	Review the memorandum of understanding between the DHS, the NSA, and USCYBERCOM for the implementation of the cyber action plan.	NSA, USCYBERCOM **(U)**

(U) Note: Action items reviewed by the team are denoted by an asterisk (*) at the end of the description.

(U) Source: 2015 Memorandum of Understanding.

(U) Sources of Classified Information

(U) The documents listed below are sources used to support classified information within this report.

~~(S//REL)~~ Source 1: [redacted]

(U) Declassification Date: September 27, 2043
(U) Generated Date: October 5, 2018

~~(S//REL)~~ Source 2: [redacted]

(U) Declassification Date: January 31, 2045
(U) Generated Date: January 16, 2020

~~(S//REL)~~ Source 3: [redacted]

(U) Declassification Date: November 30, 2043
(U) Generated Date: November 30, 2018

(U) Management Comments

(U) Office of the Deputy Secretary of Defense Comments

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAY 24 2021

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) Review of DoD Inspector General "Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations" (D2019-D000CT-0176.000) Draft Report

(U) This is the Deputy Secretary of Defense response to the DoD Inspector General Report, "Audit of DoD Implementation of the Memorandums Between the DoD and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations" (D2019-D000CT-0176.000) Draft Report.

DoD IG RECOMMENDATION 1.a: (U) We recommend that the Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff direct the DoD co-chairs of the Joint DoD-Department of Homeland Security Cyber Protection and Defense Steering Group to work with the Department of Homeland Security co-chair of the Joint DoD-Department of Homeland Security Cyber Protection and Defense Steering Group to:

a. (U) Develop and approve plans of action and milestones for each line of effort.

DoD RESPONSE 1.a: (U) DoD concurs with comment to the DoD IG recommendation. Since the publication of the 2018 joint memorandum, the practiced and ongoing collaboration among DoD, DHS, and other Federal departments and agencies reflect an improved ability for an interagency response to, and planning for, protection of domestic critical infrastructure. DoD will draft plans of action and milestones for the joint memorandum's lines of effort when they do not duplicate incident response efforts or NSC-directed operational planning.

DoD IG RECOMMENDATION 1.b: (U) We recommend that the Deputy Secretary of Defense and the Chairman of the Joint Chiefs of Staff direct the DoD co-chairs of the Joint DoD-Department of Homeland Security Cyber Protection and Defense Steering Group to work with the Department of Homeland Security co-chair of the Joint DoD-Department of Homeland Security Cyber Protection and Defense Steering Group to:

b. (U) Track activities executed and identify gaps that limit the DoD and the Department of Homeland Security in fully implementing all lines of effort in the 2018 memorandum.

DoD RESPONSE 1.b: (U) DoD concurs with comment to the DoD IG recommendation. Since the publication of the 2018 joint memorandum, the practiced and ongoing collaboration among DoD, DHS, and other Federal departments and agencies reflect an improved ability for an interagency response to, and planning for, protection of domestic critical infrastructure. DoD will track all collaborative activities related to protection and defense of critical infrastructure, gaps identified, and areas requiring improvements.

OSD070849-21/CMD005943-21

(U) Joint Staff Comments

UNCLASSIFIED

THE JOINT STAFF
WASHINGTON, DC

DJSM 0048-21
25 March 2021

Reply Zip Code:
20318-0300

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Audit of the Department of Defense's Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations

1. Thank you for providing an advance discussion copy of the subject Inspector General of the Department of Defense (DoD IG) report for review and comment.

2. The Joint Staff concurs in general with the DoD IG's findings. While not directly mentioned in the report, Title 10 limitations on domestic use of military personnel have historically created barriers to DoD-Department of Homeland Security cooperation in cyberspace. The 2010, 2015, and 2018 memorandums have been highly successful in resolving Title 10 concerns and paving the way forward.

3. Of the two recommendations laid out in the DoD IG report, the Joint Staff does not support establishing new, broad-ranging Plans of Action and Milestones (POA&Ms) for the six lines of effort described in the 2018 Memorandum. Substantial cross-over exists with current National Cyber Strategy lines of effort and existing POA&Ms. Establishing additional POA&Ms in a reactionary manner may result in confusion over roles and responsibilities, dilute economy of effort, and ultimately delay the very tasks the Cyber Protection and Defense Steering Group (CPD SG) was chartered to oversee.

4. We intend to convene the CPD SG and achieve interdepartmental consensus on the best way to address the concerns voiced in the DoD IG's report. Our position is that the CPD SG remains the best instrument for coordinating activities in service of the National Cyber Strategy.

5. The Joint Staff point of contact is [redacted]

WILLIAM D. BYRNE, JR., RADM, USN
Vice Director, Joint Staff

UNCLASSIFIED

(U) Acronyms and Abbreviations

AAR	After Action Report
CPD SG	Cyber Protection and Defense Steering Group
CSG	Cryptologic Services Group
DHS	Department of Homeland Security
HSPD	Homeland Security Presidential Directive
LOE	Line of Effort
NSA	National Security Agency
OUSD(P)	Office of the Under Secretary of Defense for Policy

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

~~SECRET//REL TO USA, FVEY~~

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 mark center drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~SECRET//REL TO USA, FVEY~~