

# **DHS Needs Additional Oversight and Documentation to Ensure Progress in Joint Cybersecurity Efforts**





**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

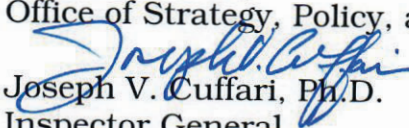
Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

November 17, 2021

MEMORANDUM FOR: Jen Easterly  
Director  
Cybersecurity and Infrastructure Security Agency

Robert Silvers  
Under Secretary  
Office of Strategy, Policy, and Plans

FROM:

  
Joseph V. Cuffari, Ph.D.  
Inspector General

SUBJECT: *DHS Needs Additional Oversight and Documentation to  
Ensure Progress in Joint Cybersecurity Efforts*

For your action is our final report, *DHS Needs Additional Oversight and Documentation to Ensure Progress in Joint Cybersecurity Efforts*. We incorporated formal comments provided by your office.

The report contains five recommendations aimed at improving the Department's cybersecurity sharing efforts. Your office concurred with all five recommendations which, based on information provided in your response to the draft report, we consider open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to [OIGAuditsFollowup@oig.dhs.gov](mailto:OIGAuditsFollowup@oig.dhs.gov).

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment





# DHS OIG HIGHLIGHTS

## *DHS Needs Additional Oversight and Documentation to Ensure Progress in Joint Cybersecurity Efforts*

**November 17, 2021**

### **Why We Did This Audit**

As cyber threats evolve, securing U.S. technology systems and networks from unauthorized access and potential exploits becomes more challenging. DHS, the National Security Agency, and the United States Cyber Command within the U.S. Department of Defense (DoD) agreed to address these challenges via a Cyber Action Plan (CAP) and memorandums. We conducted this audit to assess DHS' progress implementing the joint DHS-DoD cybersecurity efforts as required in the CAP and 2015 and 2018 memorandums.

### **What We Recommend**

We made five recommendations to improve ongoing joint efforts to implement the CAP and memorandum action items.

#### **For Further Information:**

Contact our Office of Public Affairs at (202) 981-6000, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)

### **What We Found**

The Department of Homeland Security made some progress improving cybersecurity collaboration and coordination in accordance with the CAP and memorandums. During the past 6 years, DHS participated in critical infrastructure programs, improved cyber situational awareness, co-located DHS and DoD liaisons, and conducted cybersecurity readiness training. However, we could not easily determine whether DHS had completed all requirements outlined in the CAP and memorandums because the Department did not sufficiently document the progress of its activities. Further, DHS did not effectively monitor its efforts and update its plans as required. We attribute this to DHS not establishing performance measures with milestones for completing actions, as well as inadequate staffing and governance structure to ensure its joint cybersecurity efforts remained on track. Lastly, DHS has not yet increased the number of its DoD-detailed technical staff to the level that DHS and DoD agree is appropriate to enhance cybersecurity efforts.

DHS has not fully accomplished the interagency goals of joint DHS-DoD cybersecurity efforts. Without an implementation plan that identifies milestones and progress, DHS may not be able to effectively manage its collaboration with DoD or accomplish all planned activities for protecting the Nation's critical infrastructure.

### **DHS Response**

DHS concurred with all five recommendations. We included a copy of DHS' comments in Appendix D.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

### Table of Contents

Background .....	1
Results of Audit .....	5
DHS Made Some Progress toward Improving Cybersecurity Collaboration and Coordination, but Did Not Fully Document Its Efforts .....	6
DHS Did Not Adequately Manage and Oversee Its Joint Cybersecurity Initiatives .....	9
DHS Has Not Brought on the Number of DoD Staff that DHS and DoD Agree is Appropriate to Enhance Cybersecurity Efforts.....	13
DHS Has Not Fully Accomplished Interagency Goals for Protecting Critical Infrastructure.....	14
Recommendations.....	15
Management Comments and OIG Analysis .....	15

### Appendixes

Appendix A: Objective, Scope, and Methodology .....	19
Appendix B: DHS Led 2015 CAP Objectives and Action Items .....	20
Appendix C: DHS 2018 Memorandum Lines of Effort .....	23
Appendix D: CISA Comments to the Draft Report.....	24
Appendix E: Office of Audits Major Contributors to This Report .....	29
Appendix F: Report Distribution .....	30

### Abbreviations

CAP	Cyber Action Plan
CISA	Cybersecurity Infrastructure and Security Agency
DoD	Department of Defense
EASE	Enterprise Automated Security Environment
ECD	Estimated Completion Date
iPOAM	Implementation Plan of Actions and Milestones
LOE	line of effort
NSA	National Security Agency
USCYBERCOM	United States Cyber Command



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Background

The American people increasingly depend on digital computing and connectivity for daily conveniences, essential services, and economic prosperity. Services such as electricity, finance, transportation, water, and health care are facilitated digitally, which introduces new vulnerabilities to computer systems and data. Substantial growth in Internet access and networked devices has further facilitated widespread opportunities and innovation. The protection of sensitive information from threats and the security of systems that process, store, or transmit information remain critical. Recently, efforts to protect information and information systems have included combating cyber threats against multinational Coronavirus 2019 vaccine companies and research facilities,<sup>1</sup> and the 2020 election infrastructure.

The Department of Homeland Security plays a critical role in protecting the Nation's cyber space, which includes not only DHS' own computer systems and information, but also those belonging to other Federal civilian agencies. For example, DHS is the lead government agency responsible for maintaining secure, functional, and resilient critical infrastructure.<sup>2</sup> As part of this mission, DHS coordinates and integrates information among Federal cyber operations centers, state and local governments, and the private sector.

Within DHS, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for executing DHS' cybersecurity missions. CISA is tasked with preserving the integrity of critical infrastructure and ensuring the resilience of national critical functions and civilian Federal network security from cyber and physical threats.<sup>3</sup> Each day, CISA provides crisis management, incident response, and defense against cyber attacks for Federal civil executive branch networks. The National Cybersecurity and Communications Integration Center,<sup>4</sup> which was a part of CISA, served as a central location for DHS' operational components involved in cyber response activities to share information between the public and private sectors. CISA also serves as the main Federal interface for cyber threat indicators and information sharing, and

---

<sup>1</sup> *The Hill*, "Microsoft warns Russian, North Korean hackers targeting groups researching COVID-19 vaccines," November 13, 2020.

<sup>2</sup> There are 16 critical infrastructure sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare/Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; and Water/Wastewater Systems.

<sup>3</sup> *National Cybersecurity and Communications Integration Center: Department of Defense Support to the Department of Homeland Security Concepts of Operations, Version 3*, November 2018.

<sup>4</sup> In June 2020, CISA consolidated and integrated the functions of the National Cybersecurity and Communications Integration Center into its new CISA Central.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

provides services and programs to reduce and mitigate the risk of catastrophic consequences stemming from cyber attacks.

### **Cybersecurity Coordination between DHS and the Department of Defense**

Coordination with the Department of Defense (DoD) is vital for securing cyberspace and Federal/private sector networks. Because of the importance of information technology systems supporting critical infrastructure, DHS has determined that a large-scale cyber incident or combination of incidents could exceed its own incident response support capacity. As the Nation's military force, DoD must ensure the U.S. military's ability to fight, win wars, and project power while under attack in any domain, including cyberspace. DoD's mission includes preempting, defeating, or deterring malicious cyber activity that targets U.S. critical infrastructure — activity that may cause a significant cyber incident.<sup>5</sup> DoD also supports efforts to defend the Defense Industrial Base critical infrastructure sector networks and systems from malicious cyber activity that could undermine U.S. military strength. In turn, through coordination with DHS, DoD benefits from a greater understanding of how to address risks stemming from dependencies on non-DoD-owned critical infrastructure.

Within DoD, the United States Cyber Command (USCYBERCOM)<sup>6</sup> and the National Security Agency (NSA)<sup>7</sup> collaborate to provide cybersecurity support through their respective missions. USCYBERCOM directs, synchronizes, and coordinates cyberspace planning and operations to defend and advance national interests with domestic, interagency, and international partners. NSA leads the U.S. Government in cryptology, which includes signal intelligence, information assurance, and cybersecurity. NSA and USCYBERCOM share the same command, with USCYBERCOM depending on NSA's workforce, computer networks, and intelligence to operate.

Recognizing the need for greater cybersecurity collaboration, the Secretaries of Homeland Security and Defense have established formal agreements via three primary memorandums during the past 10 years to enhance interagency communication and synchronize operational and incident response activities. In 2010, DHS and DoD established a memorandum of agreement<sup>8</sup> that encouraged joint focus on national cybersecurity efforts, increasing the overall

---

<sup>5</sup> 2018 *Department of Defense Cyber Strategy*.

<sup>6</sup> USCYBERCOM is a national unified combatant command under DoD.

<sup>7</sup> NSA is a national-level intelligence agency of DoD, under the authority of the Director of National Intelligence.

<sup>8</sup> *Memorandum of Agreement between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity*, September 27, 2010.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

capacity and capability of both DHS' homeland security and DoD's national security missions. The memorandum of agreement was intended to increase interdepartmental collaboration in strategic planning for the Nation's cybersecurity, provide mutual support for cybersecurity capabilities development, and synchronize operational cybersecurity missions.

In 2015, DHS, NSA, and USCYBERCOM developed a memorandum of understanding<sup>9</sup> to establish and maintain a Cyber Action Plan (CAP) to implement provisions of the 2010 memorandum of agreement. The stated purpose of the CAP was to generate a community of trust and increase the security and resilience of the Nation's critical infrastructure. The CAP was intended to enhance interagency collaboration and cooperation through specific goals, objectives, and action items, outlined in Appendix A of the 2015 memorandum of understanding.

In 2018, the Secretary of Homeland Security and the Secretary of Defense established a joint memorandum<sup>10</sup> to clarify the roles and responsibilities between DHS and DoD and enhance the U.S. Government's readiness to respond to cyber threats. To accomplish this, the 2018 joint memorandum established six coordinated lines of effort (LOE) to secure, protect, and defend the homeland. These LOEs were:

1. Intelligence, Indicators, and Warning
2. Strengthening the Resilience of National Critical Functions
3. Increasing Joint Operational Planning and Coordination
4. Incident Response
5. Integrating with State, Local, Tribal, and Territorial Governments
6. Defense of Federal Networks

See Appendix C for the list of LOEs and whether the Office of Inspector General identified efforts to complete them.

Figure 1 summarizes the three memorandums between DHS and DoD.<sup>11</sup>

---

<sup>9</sup> *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 24, 2015.

<sup>10</sup> *Joint DoD-DHS Memorandum on the Protection and Defense of Critical Infrastructure*, October 6, 2018.

<sup>11</sup> For simplicity, in this report, we refer to the 2010 memorandum of agreement, 2015 memorandum of understanding, and 2018 joint DHS-DoD memorandum all as memorandums.

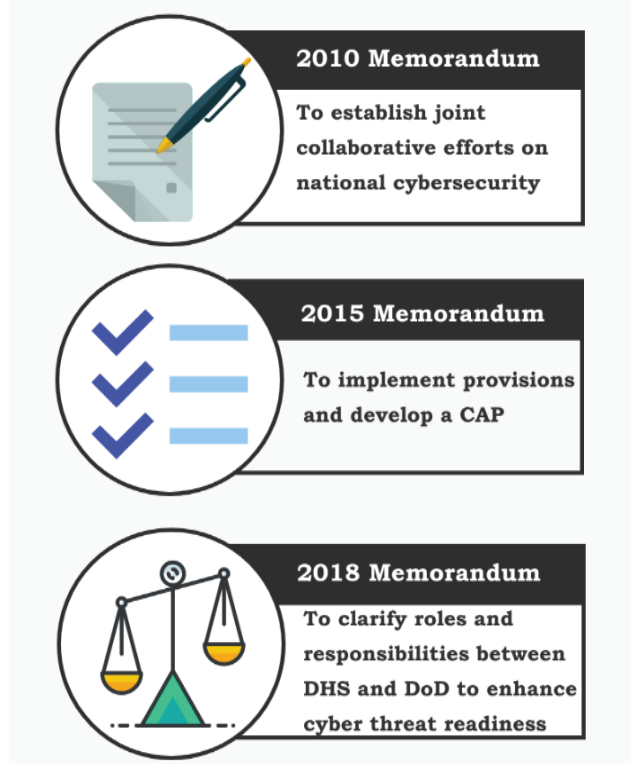




## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

**Figure 1. DHS-DoD CAP-Associated Memorandums**



Source: DHS OIG-generated

### **DHS/NSA/USCYBERCOM CAP**

The CAP includes 3 interagency goals and 13 objectives intended to leverage the unique knowledge, capabilities, and comparative advantages of each organization. The three interagency goals are to:

1. Increase the level of protection and defense of U.S. critical infrastructure.
2. Increase Federal government cybersecurity/shared situational awareness.
3. Increase interagency coordination and operational integration to enhance prevention and mitigation of, response to, and recovery from domestic cybersecurity incidents.

The CAP outlines 32 associated action items. Although the CAP does not include milestones or deadlines, it does identify agencies' responsibility for tracking progress of the action items. DHS is responsible for executing and tracking the progress of 21 of the 32 action items. See Appendix B for a full list of these action items and whether OIG identified DHS efforts to complete them.





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

The 2015 memorandum includes instructions for implementing the detailed requirements, roles, and responsibilities outlined in the 2010 memorandum. For DHS, CISA<sup>12</sup> is to adhere to the most current version of the CAP, periodically review its content, make appropriate recommendations for updates, and fully participate in the governance processes.

The 2015 memorandum also outlines a governance structure consisting of an Executive Committee instructed to meet at least semi-annually and a Steering Committee that is to meet at least quarterly. The Executive and Steering Committees (Committees) are to consist of representatives from DHS, NSA, and USCYBERCOM, who are sufficiently senior, to ensure effective oversight of the CAP. The 2018 memorandum further requires its steering group to report on progress and challenges implementing the activities, initiatives, and efforts twice annually.

We conducted this audit to assess DHS' progress implementing the joint DHS-DoD cybersecurity efforts as required in the CAP and the 2015 and 2018 memorandums.

### Results of Audit

DHS made some progress to improve cybersecurity collaboration and coordination in accordance with the CAP and memorandums. Specifically, during the past 6 years, DHS participated in critical infrastructure programs, improved cyber situational awareness, co-located DHS and DoD liaisons, and conducted cybersecurity readiness training. However, we could not easily determine the extent to which DHS completed all requirements outlined in the CAP and memorandums because the Department did not sufficiently document the progress of its activities. Further, DHS did not effectively monitor its efforts and update its plans as required. We attribute this to DHS not establishing performance measures with milestones for completing actions, as well as to inadequate staffing and governance structure to ensure its joint cybersecurity efforts remained on track. By law, DoD is authorized to detail or assign as many as 50 cybersecurity technical personnel to DHS within any fiscal year.<sup>13</sup> DoD has indicated its initial intent to provide 20 such personnel,<sup>14</sup> an amount that DHS agrees is appropriate to enhance cybersecurity efforts. Despite this, DHS has not yet brought on DoD cybersecurity technical personnel at this agreed-upon level.

---

<sup>12</sup> CISA is the successor to the National Protection and Programs Directorate, which was the DHS signatory to the 2015 memorandum.

<sup>13</sup> *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Public Law 115-232, §1650, August 13, 2018, referred to as Section 1650.

<sup>14</sup> *DoD Implementation of Section 1650 of the National Defense Authorization Act for Fiscal Year 2019*.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

As of July 2020, DHS had only 10 DoD personnel onboard, each of whom was serving a 6-month detail.

DHS has not fully accomplished the interagency goals of the joint DHS-DoD efforts. Without an implementation plan that identifies milestones and progress, DHS may not be able to effectively manage its collaboration with DoD or accomplish all planned activities for protecting the Nation's critical infrastructure.

### **DHS Made Some Progress toward Improving Cybersecurity Collaboration and Coordination, but Did Not Fully Document its Efforts**

During the past 6 years, DHS made progress toward improving cybersecurity collaboration and coordination with NSA and USCYBERCOM. However, the Department could not demonstrate completion of specific initiatives it had undertaken. We were unable to confirm completion of these efforts because DHS had not sufficiently documented the progress of each activity.

### **DHS Took Steps to Improve Cybersecurity Collaboration and Coordination**

DHS initiated four key cybersecurity efforts in support of the CAP and the 2015 and 2018 memorandums to (1) participate in critical infrastructure programs, (2) improve cyber situational awareness, (3) co-locate DHS and DoD liaisons, and (4) perform cybersecurity readiness training and exercises.

#### Participation in Critical Infrastructure Programs

DHS enhanced DoD-DHS information sharing with the private sector for two critical infrastructure areas. The U.S. Government and the private sector work closely on the security and resilience of critical infrastructure through a public-private relationship model — initiatives referred to as Pathfinder programs are one aspect of this model. Each Pathfinder program is meant to address the technologies, challenges, and threats facing a critical infrastructure sector.

DHS participated in two Pathfinder programs during the past 2 years that were focused on the Energy and Financial Services critical infrastructure sectors. According to DHS officials, these Pathfinder efforts have been effective. Specifically, the Energy sector Pathfinder advanced threat information sharing, improved training and education to understand systemic risks, and developed joint operational preparedness and response activities. The Financial Services sector Pathfinder program enhanced security and resilience of the sector's critical infrastructure and reduced operational risks. DHS is leading two



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

additional initiatives: (1) a malware sharing initiative to allow for the sharing of declassified malware information with trusted partners, and (2) a mutual interest initiative to operationalize cyber threat information sharing.

#### Improving Cyber Situational Awareness

DHS initiated and implemented a cross-government Multilateral Information Sharing Agreement in 2015,<sup>15</sup> which was updated in 2019, to enhance cybersecurity information sharing among Federal agencies.<sup>16</sup> This agreement established three roles of Federal information-sharing participants: (1) as data producers, (2) data consumers, and/or (3) shared capability providers who work collaboratively on information sharing across the Government. The participants agreed to exchange cybersecurity information about incidents, malware, and threat actors as part of their respective cybersecurity missions.

#### Exchanging and Co-locating DHS and DoD Liaisons

In keeping with the long-standing practice of exchanging liaisons between DoD and DHS, DoD provided 11 liaisons to DHS. In June 2019, DHS also co-located three liaisons at DoD. Liaisons, who are DoD and CISA cyber analysts, facilitate coordination and further the work of both departments on issues related to homeland security, homeland defense, civil support, and other missions and issues of mutual interest. Together, they facilitate situational awareness, coordinate engagement activities, standardize threat detection efforts, and identify opportunities for synchronizing interdepartmental missions.

#### Performing Cybersecurity Readiness Training and Exercises

DHS participated in cybersecurity preparedness training to improve readiness for national security risks. Specifically, DHS participated in 46 joint national-level cyber trainings and exercises, of which it led 3, between 2015 and 2019. As part of this training, participating organizations responded to simulated attacks by practicing response policies and procedures. These exercises allow the cyber incident response community to identify relative strengths and interdependencies, practice and measure the effectiveness of their capabilities, and continuously improve incident response processes. They also strengthen information sharing partnerships among Federal, state, international, and

---

<sup>15</sup> *Enhance Shared Situational Awareness Multilateral Information Sharing Agreement*, March 2015, which was renamed *Federal Multilateral Information Sharing Agreement*, January 2019.

<sup>16</sup> As of June 2018, 36 Federal departments and agencies signed the agreements.

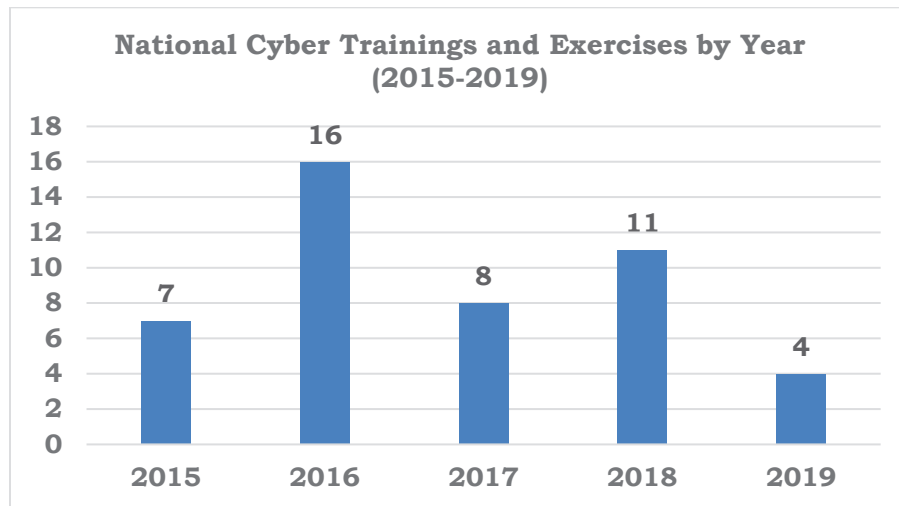


## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

private sector partners. Figure 2 shows the number of national cyber trainings and exercises in which DHS participated from 2015 to 2019.

**Figure 2. DHS-Involved National Cyber Trainings and Exercises**



Source: DHS OIG analysis based on CISA data

### DHS Could Not Demonstrate Completion of Cybersecurity Initiatives

Although DHS has taken steps to improve cybersecurity collaboration and coordination, at the time of our audit it had not yet completed all 13 objectives required in the CAP. For example, DHS had not yet:

- developed measures of effectiveness and performance on exchange of cyber indicators to determine trends, identify areas for improvement, and implementation strategy;
- established cross-organization analytical capabilities that enable analysts and operators to share results and support synchronized operational actions;
- identified potential or anticipated departmental capability and resource gaps during significant domestic cyber incident response activities to obtain DoD's support and assistance; or
- finalized the pre-decisional draft of the *DoD-DHS Memorandum, "Critical Infrastructure Defense/Protection Collaboration" Implementation Plan of Actions and Milestones*, despite it being initiated a month after the signing of the 2018 memorandum.

Further, DHS was not able to demonstrate completion of specific activities outlined in the CAP or to meet the intent of the 2015 and 2018 memorandums. The CAP requires DHS to close out the memorandums in writing to ensure





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

completion of cybersecurity efforts. However, CISA was not able to provide documentation proving activities were completed. We made numerous requests during this audit for such documentation, but CISA officials stated they had not recorded the details of the specific efforts underway.

#### **Cybersecurity Initiatives Were Not Well Documented**

We were unable to confirm completion of specific activities outlined in the CAP and the 2015 and 2018 memorandums because CISA did not sufficiently document the progress of each activity. Near the completion of this audit, CISA drafted a white paper<sup>17</sup> as an informal attempt to summarize its past and current initiatives. The white paper described dozens of current and past initiatives to meet the intent of the 2015 and 2018 memorandums. For example, the white paper described coordination for vulnerability disclosures and mitigation directives for systems and network devices, campaign coordination to issue joint product efforts and counter cyber and malware attacks, election security initiatives, and Coronavirus 2019 protection efforts. However, we were not able to determine the number of initiatives completed compared to the number still underway at the time of this audit.

Although the white paper was useful to indicate the number of initiatives underway, CISA could not identify or confirm the start or end date for each effort. Specifically, the white paper did not show any form of closeout or progress related to the 2015 and 2018 memorandums. CISA also did not provide documentation to show whether any of the initiatives underway had met the intent of the 2015 and 2018 memorandums. In comparing the white paper to the memorandums, it was not clear when past initiatives and activities were completed satisfactorily or whether they had evolved over time. Consequently, we could not identify or verify the status (i.e., closed, open, terminated, or removed) of each task or activity in the memorandums.

#### **DHS Did Not Adequately Manage and Oversee Its Joint Cybersecurity Initiatives**

DHS did not effectively monitor progress or complete annual updates on CAP action items and associated 2015 and 2018 memorandums as required. We attribute this to DHS not finalizing performance measures and not establishing milestones for completing actions, and inadequate staffing and governance structure to ensure its joint cybersecurity efforts remained on track.

---

<sup>17</sup> *Overview of Activities Under the DoD-DHS MOU for 2015 and 2018*, July 7, 2020.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

#### **DHS Did Not Periodically Assess or Update Memorandums as Required**

DHS did not effectively monitor progress and complete annual updates on CAP action items and associated 2015 and 2018 memorandums as required. According to the 2015 memorandum, DHS was required to periodically review its content, make appropriate recommendations for updates, and fully participate in the governance process. However, we determined that DHS did not conduct periodic assessments to measure completion of the specific goals, objectives, and required action items in the CAP and memorandums. We requested evidence supporting completion of CAP activities or updates to a current version of the CAP, but CISA stated it had not recorded the details of the specific efforts underway. Without evidence of periodic assessments or an implementation plan, coordination and collaboration, we could not determine the status of the memorandums' requirements and activities.

DHS acknowledged it did not have enough staff to document, track, and maintain ongoing CAP activities. CISA officials stated they did not have the staffing resources or measures to centrally track the memorandums' activities. CISA officials also explained that staffing turnovers from previous years continued to hinder ongoing efforts. In its fiscal year 2020 *DHS Cybersecurity Strategy Implementation Plan*, the Department acknowledged that fully resourcing identified cybersecurity goals and objectives remains a significant challenge within current budget constraints. The FY 2020 DHS plan also notes that additional resources are needed to accomplish identified outcomes. DHS also acknowledged that it does not have a central repository to track and store supporting documents for the memorandums.

#### **DHS Did Not Finalize Performance Measures and Establish Milestones**

Performance measures indicate whether a program is meeting its goals and achieving expected results and address the products and services a program delivers, as well as the results of those products and services. However, at the time of our audit, DHS had not finalized performance measures to direct or monitor its efforts to accomplish the tasks and activities outlined in the 2015 and 2018 memorandums. By not formalizing performance measures needed to direct or monitor its efforts to accomplish the tasks and activities in the 2015 and 2018 memorandums, DHS could not report the accomplishments of the activities.

DHS also did not finalize a plan that established milestones for completing action items. In October 2018, the Department began a pre-decisional draft *Implementation Plan of Actions and Milestones* (iPOAM). DHS intended for the iPOAM to establish specific, outcome-based interagency collaboration by



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

further clarifying roles and responsibilities between DHS and DoD. The draft iPOAM lists action items for each LOE, with columns identifying the lead, support, and suspense information for each action item. Governance and oversight of the iPOAM included a working group that was to meet as frequently as needed, to conduct status updates and review the document. In addition, oversight of iPOAM included the working group reporting to the Secretary of Defense and the Secretary of Homeland Security twice annually on DHS' progress of action items and challenges. In May 2020, a CISA official stated that the working group was waiting to coordinate with the DHS Office of Policy to finalize the iPOAM because of competing priorities. Consequently, the iPOAM had not been finalized. Based on this information, we determined that DHS did not make assigning staff to monitor memorandum progress a priority.

Although the iPOAM mirrored the joint principles in the 2018 memorandum, DHS and DoD officials stated that the iPOAM did not allow flexibility. According to DoD officials, although DHS and DoD both provided input to prioritize action items, they change as events occur in real time. According to DHS and DoD officials, both departments communicated challenges and progress more than twice per year. However, OIG did not obtain evidence of these challenges or of a plan of action to resolve or address them, as CISA officials said it had not recorded the details of the specific efforts underway. Further, at the time of this audit, the iPOAM working group had been inactive. CISA personnel said the working group effort was overcome by other events.

Finally, CISA could have leveraged from DHS reporting mechanisms to capture the performance measures and milestones. For example, DHS issued its *Office of Cybersecurity and Communications*<sup>18</sup> *FY 2018 Strategic Intent*,<sup>19</sup> and the *DHS Cybersecurity Strategy Implementation Plan* for FY 2018 and 2020.<sup>20</sup> These documents call for CISA to increase collaboration with its partners in reducing national systemic and catastrophic cyber risks. They did not, however, reference the CAP and associated memorandums' performance measures and activities.

---

<sup>18</sup> The Office of Cybersecurity and Communications, previously within the former National Protection and Preparedness Directorate, was responsible for enhancing the security, resiliency, and reliability of the Nation's cyber and communication infrastructure.

<sup>19</sup> The strategic intent identified seven goals to expand and enhance the Nation's overall security and resilience.

<sup>20</sup> The cybersecurity strategy implementation plans identify seven goals to help make cyberspace secure and resilient.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### **Governance Structure Was Not Fully Effective**

The 2015 memorandum outlines requirements for a governance structure consisting of an Executive Committee instructed to meet at least semi-annually and a Steering Committee that would meet at least quarterly. These Committees are to consist of representatives from DHS, NSA, and USCYBERCOM. DHS representatives on the Committees include members from CISA and the Office of Policy. However, according to DHS Office of Policy officials, they had very limited engagement with CISA on its efforts to implement the 2015 memorandum. This is because the 2015 memorandum was in place prior to the Office of Policy's involvement in component-level cyber-related efforts.

In 2016, DHS established a Cyber Action Plan Implementation Team to serve as the mechanism and structure for ensuring progress toward completion of objectives and action items identified in CAP.<sup>21</sup> DHS also designated a Cyber Action Plan Implementation Secretariat to maintain the most current version of the CAP in a central location accessible to all members. Although DHS established this Team and designated the Secretariat, we determined that the Department did not monitor progress toward completing the CAP objectives and action items.

DHS was not fully successful in its efforts to establish a governance structure to monitor and implement the 2018 memorandum action items. DHS and DoD established a Steering Group in 2018 to set priorities and collaborate on improving the protection and defense of critical infrastructure, and to enhance cyber threat response readiness. Part of this work called for reporting on the progress and challenges implementing the joint cybersecurity efforts in the 2018 memorandum.<sup>22</sup> DHS officials stated that progress for action items in the 2018 memorandum are monitored through quarterly Steering Group meetings and the outcomes of those meetings are documented in the meeting minutes. We requested meeting minutes from the Steering Group's quarterly meetings from 2015 through 2020, but DHS did not have documentation to demonstrate that meetings were held regularly during that time. The Steering Group also did not address or provide the status of all tasks and activities outlined in the 2018 memorandum. Furthermore, through its 2018 charter, the Steering Group was tasked with prioritizing the six LOEs and approving a plan of action and milestones for each. However, DHS could not provide any evidence to support monitoring and implementation of the 2018 memorandum.

---

<sup>21</sup> *Charter for Cyber Action Plan Implementation Team*, April 15, 2016, referred to as the 2016 Charter.

<sup>22</sup> *Joint Department of Defense-Department of Homeland Security Cyber Protection and Defense Steering Group Charter, Version 2.5*, November 2018.





## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

We met with DoD officials who stated their focus was on the outcome of the 2018 memorandum. Additionally, DoD officials did not believe it was necessary to have a process for formal reporting and wanted to minimize unnecessary burdens. They reiterated that the memorandums' value was to build relationships and trust, as well as to gain understanding of each department's needs. DoD officials also stated they would be hesitant to use another memorandum if it required having specific milestones.

### **DHS Has Not Brought on the Number of DoD Staff that DHS and DoD Agree is Appropriate to Enhance Cybersecurity Efforts**

To execute terms of the 2018 memorandum, the Secretary of Defense, in coordination with the Secretary of Homeland Security, is authorized to provide, detail, or assign as many as 50 cybersecurity technical personnel to DHS within any fiscal year, with the option to extend for an additional year.<sup>23</sup> This arrangement is intended to enhance cybersecurity cooperation, collaboration, and unity of Government efforts. In July 2020, DoD issued guidance limiting the number to a maximum of 20 personnel, subject to increase based on review.<sup>24</sup> As of August 2020, DHS had 10 DoD personnel who were each serving a 6-month detail. According to CISA officials, the detailed personnel started with DHS in September 2020 — two were assignees and eight were detailees. The assignees were tasked to provide intelligence support, and the detailees were tasked to integrate into incident response teams.

Additionally, DHS and DoD completed a memorandum of agreement<sup>25</sup> in 2020 that outlined the provisions for detailing or assigning DoD technical personnel to DHS for enhancing cybersecurity cooperation, collaboration, and unity of Government efforts. The memorandum of agreement specifically addresses the general activities to be performed by the detailed or assigned DoD personnel — operational and administrative control; information-handling requirements, responsibilities, and functions; and start and end dates. The memorandum of agreement also provides the mechanism for DoD to gain greater understanding of, and ability to address risks that arise from its dependencies on non-DoD-owned critical infrastructure essential to its forces and operations.

---

<sup>23</sup> Section 1650 limits the authority to the provision of no more than 50 personnel within any fiscal year. It does not specify length of assignment or details for specific personnel or the ability to extend assignments/details.

<sup>24</sup> DoD Implementation of Section 1650 of the National Defense Authorization Act for Fiscal Year 2019.

<sup>25</sup> Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Assignment or Detail of Cybersecurity Personnel, July 20, 2020.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

The exchange of personnel is a key part of increasing collaboration and the overall capacity and capability of both DHS' homeland security and DoD's national security missions. According to DHS officials, the Department is refining its approach so DoD can best support surge capacity and other areas, such as classified projects and election security. DHS is also defining how best to leverage DoD's expertise in planning and transportation areas, to assist other components (e.g., Transportation Security Administration and United States Coast Guard). Additionally, DHS officials emphasized that the Coronavirus-19 pandemic has hindered efforts to determine support needed because some DoD personnel detailed to DHS were also engaged in pandemic response efforts, which negatively affected the timeline to onboard additional staff.

### **DHS Has Not Fully Accomplished Interagency Goals for Protecting Critical Infrastructure**

DHS has not completed the three interagency goals and 13 objectives laid out in the CAP and memorandums. The three interagency goals were intended to increase the level of protection and defense of U.S. critical infrastructure; increase Federal government cybersecurity/shared situational awareness; and increase interagency coordination and operational integration to enhance prevention and mitigation of, response to, and recovery from domestic cybersecurity incidents. The 32 action items outlined in the CAP were intended to increase the security and resilience of U.S. critical infrastructure and build consistency to strengthen cybersecurity collaboration. By not accomplishing its goals, DHS may not receive the adequate level of assistance from DoD to conduct joint operations to protect critical infrastructure; support key stakeholders; and jointly defend civilian and military networks from cyber threats. Incomplete action items may also increase the risk of redundant cybersecurity activities and efforts.

Also, until DHS establishes an implementation plan that identifies and documents milestones, completion dates, and progress, DHS may not be able to effectively manage its collaboration with DoD. Delays in progress may hamper information sharing and impair day-to-day cybersecurity and incident response operations. Likewise, until DHS fully leverages the allocation of cybersecurity resources from DoD, it will not be able to effectively collaborate and coordinate cybersecurity mitigation efforts. Having DoD technical cybersecurity personnel staff levels be lower than what DoD has allocated and Congress has authorized reduces cybersecurity cooperation, collaboration, and unity of U.S. Government efforts. Full allocation of technical staff will provide mutual benefits to the departments by facilitating exchange and leverage of



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

knowledge and tradecraft, improving the ability to operate jointly, improving collective cybersecurity capabilities, and enhancing information sharing.

### Recommendations

**Recommendation 1:** We recommend the Director of CISA develop an implementation plan to conduct periodic assessments for monitoring the progress of goals and activities and complete annual updates on action items, as required by the Cyber Action Plan and associated 2015 and 2018 memorandums.

**Recommendation 2:** We recommend the Director of CISA conduct centralized tracking and completion of signed closeout summaries to reconcile the ongoing, outstanding, and open tasks and activities, as required by the Cyber Action Plan and associated 2015 and 2018 memorandums.

**Recommendation 3:** We recommend the Director of CISA establish performance measures to ensure the effectiveness and completion of the Cyber Action Plan and associated 2015 and 2018 memorandum activities.

**Recommendation 4:** We recommend the Director of CISA establish the DHS governance structure and ensure it consists of an Executive Committee that meets at least semi-annually and a Steering Committee that meets at least quarterly, as required.

**Recommendation 5:** We recommend the Under Secretary, Office of Strategy, Policy, and Plans establish a plan, in coordination with CISA, for the appropriate allocation of technical personnel to ensure DHS-DoD effective coordination and collaboration efforts.

### Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Department. In its comments, the Department stated it appreciated the work of OIG in planning, conducting its review, and issuing this report.

We have reviewed the Department's comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. All five recommendations are open and resolved. A summary of the Department's responses and our analysis follows:



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

**DHS Response to Recommendation #1:** Concur. CISA's Cybersecurity Division and the DHS Office of Strategy, Policy, and Plans jointly represent DHS as co-chairs of the DoD-DHS Cyber Protection and Defense Steering group, as established by the "Joint DoD-DHS Memorandum on the Protection and Defense of Critical Infrastructure," dated October 6, 2018. Going forward, CISA's Cybersecurity Division — with support from the CISA Office of Strategy, Policy, and Plans, and in coordination with DHS Office of Strategy, Policy, and Plans and DoD co-chairs — will develop an implementation plan to address the unresolved action goals, activities, and action items in the 2015 CAP, as well as the associated November 2015 and October 2018 memorandums. This effort will include conducting periodic assessments and annual updates for remaining and future goals, activities, and action items. Estimated Completion Date (ECD): March 31, 2022.

### OIG Analysis of DHS Comments

DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

**DHS Response to Recommendation #2:** Concur. CISA's Cybersecurity Division, with support from CISA's Office of Strategy, Policy, and Plans, and in coordination with DHS Office of Strategy, Policy, and Plans, will take steps to establish and implement a centralized tracking capability to maintain visibility and ensure progress of open action items established between DoD and DHS within the CAP and the 2015 and 2018 memorandums, as well as reconcile incomplete actions and tasks. These actions include establishing and formalizing a centralized secretariat function to track tasks and activities; conducting a thorough review of goals, activities, and action items for completeness and relevancy of continued work efforts; carrying relevant and incomplete action items in a new Plan of Actions and Milestones; closing out completed or irrelevant action items through documented and signed "close out summaries"; and coordinating with DoD to formally "close out" the 2015 memorandum and CAP. ECD: December 31, 2021.

### OIG Analysis of DHS Comments

DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

**DHS Response to Recommendation #3:** Concur. CISA's Cybersecurity Division, in coordination with DHS Office of Strategy, Policy, and Plans, will





## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

work with CISA's Office of the Chief Financial Officer, Program Analysis & Evaluation Division, to establish and implement performance metrics applicable to the 2015 CAP and associated 2015 and 2018 memorandum activities. Once implemented, performance metrics will be used to maintain visibility of progress and to measure effectiveness and completion.

Performance metrics for active action items will be reviewed quarterly by CISA and DHS chairs of the DoD-DHS Cyber Protection and Defense Steering Group to ensure continued visibility and to implement formal inject points for senior level guidance as needed. ECD: March 31, 2022.

### **OIG Analysis of DHS Comments**

DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

**DHS Response to Recommendation #4:** Concur. CISA's Cybersecurity Division, with support from CISA's Office of Strategy, Policy, and Plans, and in coordination with DHS Office of Strategy, Policy, and Plans and DoD co-chairs, will review and clarify the DHS structure under which active DoD-DHS memoranda and plans will be governed. The 2015 and 2018 memoranda prescribe different governance structures, which have not been fully reconciled. Additionally, significant reorganization has taken place within CISA and DHS since the development of the 2015 memorandum and its governance structure. Accordingly, CISA's Cybersecurity Division and DHS Office of Strategy, Policy, and Plans will review prescribed structures and formally establish, and adhere to, a governance structure appropriate and effective for the Department given its current organizational structure. ECD: March 31, 2022.

### **OIG Analysis of DHS Comments**

DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

**DHS Response to Recommendation #5:** Concur. In August 2020, DHS Office of Strategy, Policy, and Plans and CISA provided DoD a prioritized request that would have fully implemented the 50-person accompaniment authorized by Section 1650 of the *2019 National Defense Authorization Act*. DHS Office of Strategy, Policy, and Plans and CISA, in coordination with other operational DHS components, will seek to reaffirm that prioritized request and will continue to work with DoD counterparts through the DoD-DHS Cyber Protection and Defense Steering Group to advocate for additional allocation of



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

DoD technical personnel in support of joint DHS/DoD priorities. This work will continue through September 30, 2022, at which point the pilot program established under Section 1650 of the *2019 National Defense Authorization Act* is no longer authorized. ECD: September 30, 2022.

### **OIG Analysis of DHS Comments**

DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

## Appendix A

### Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*.

The objective of this audit was to assess DHS' progress implementing the joint DHS-DoD cybersecurity efforts, as required in the CAP and 2015 and 2018 memorandums. As part of this audit, we sought to determine whether DHS has:

- coordinated with NSA and USCYBERCOM to perform the roles and responsibilities outlined under various agreements;
- established with DoD processes and systems used to analyze and share cyber threat information with the critical infrastructure owned or operated by state, local, tribal, and territorial governments; and
- monitored the effectiveness, completion, and compliance of its performance in meeting goals and objectives outlined in the 2015 and 2018 memorandums.

We conducted this audit as a joint effort with the DoD OIG. However, we performed limited joint fieldwork with DoD OIG because of the COVID-19 pandemic. Our fieldwork consisted of interviewing selected personnel from DoD, DHS, and CISA. Additionally, we reviewed applicable policies, procedures, published reports, documents, testimonies, and media articles pertaining to the sharing of cyber threat information pursuant to CAP and memorandums agreed upon by DHS, NSA, and USCYBERCOM. We also reviewed joint national-level cyber training exercises and information-sharing agreements and procedures.

We conducted this performance audit between January 2020 and October 2020 pursuant to the *Inspector General Act of 1978, as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Appendix B**  
**DHS-Led 2015 CAP Objectives and Action Items**

The DHS OIG audit team reviewed and analyzed documents supporting DHS and CISA efforts to implement action items identified in the CAP. The following table highlights details on the action items and whether we identified efforts to complete them.

<b>DHS-Led 2015 CAP Objectives and Action Items</b>	<b>Efforts Identified by OIG</b>
<b>Objective 1.3</b> Develop measures of effectiveness and performance on the quantity and quality of exchange of signatures and indicators among DHS, NSA, and USCYBERCOM with the ultimate objective of real-time transfer using Information Sharing Architecture capabilities, as appropriate, at all classification levels.	Yes
<b>1.3.1</b> Develop performance measures including measuring current delivery rate, information quality, and effectiveness from the moment of incident detection, through the point at which the agency is informed of the incident, to final implementation.	Yes
<b>1.3.2</b> Develop measures of effectiveness and assess transmitted indicators exchanged among agencies in order to determine measurement trends, identify areas for improvement, and implement identified improvements to enhance performance.	Yes
<b>Objective 1.4</b> 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.	Yes
<b>1.4.1</b> Develop an analytical framework (i.e., information sharing language/taxonomy) for the exchange of cyber tactics, techniques, and procedures and tradecraft consistent with Information Sharing Architecture profiles agreed to by the Federal Cyber Centers.	Yes
<b>1.4.2</b> Establish initial capabilities that enable the results of "local" analytics to be shared among operations centers using Information Sharing Architecture profiles.	Yes
<b>Objective 1.5</b> Resolve when practical policy and legal impediments inhibiting information sharing and develop remedial solutions as appropriate to enable more timely and effective cybersecurity protection and defense of U.S. critical infrastructure, and where possible, leverage existing enabling efforts (e.g., Information Sharing Architecture Access Control Specification and the Enhance Shared Situational Awareness Multilateral Information Sharing Agreement).	No
<b>1.5.1</b> Select appropriately scoped and analyzed use-case scenarios to determine the flow of information (quality and quantity) between DHS,	No





**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

NSA, and USCYBERCOM to identify potential impediments, gaps and solutions to policy and legal issues inhibiting effective interagency collaboration.	
<b>1.5.2</b> Leverage use-case scenario analysis to develop remedial solutions as appropriate, such as the automatic deployment of countermeasures or other means, to more rapidly and effectively protect and defend U.S. critical infrastructure.	No
<b>Objective 2.3</b> 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 (EASE) efforts and offering customizable levels of semi-automated and automated decision-making processes that can be used for National Security Systems and non-National Security Systems Federal and private sector applications.	Yes
<b>2.3.1</b> Develop technical concepts and roadmaps relating to EASE.	Yes
<b>2.3.2</b> Work with the National Institute of Standards and Technology to identify opportunities in developing specific standards relating to EASE.	Yes
<b>2.3.3</b> Develop a Joint EASE Reference Architecture and Reference Requirements Set to enable coordinated engagement with vendors and joint capability development.	Yes
<b>2.3.4</b> Explore opportunities for joint research and technology assessment activities relating to EASE, including leveraging the Department of Energy National Labs to create an enduring supply of cybersecurity ideas and researched prototypes.	Yes
<b>2.3.5</b> Explore opportunities for joint engagement with industry and academia relating to EASE and plan joint EASE-related pilots in accordance with all applicable laws, regulations, and policies.	Yes
<b>Objective 3.1</b> Perform interagency training and exercises to increase shared awareness of operational capabilities and to enhance coordination, mitigation, and response to cybersecurity incidents.	Yes
<b>3.1.1</b> Identify and resolve resourcing, planning, and policy issues that inhibit full organizational participation as appropriate in large-scale cyber exercises (e.g., Cyber Guard, Cyber Storm, and National Level Exercises).	Yes
<b>3.1.2</b> Ensure proper representation and participation in cyber exercise After Action Reports and establish formal mechanisms for integrating findings and recommendations into management processes for resolution.	Yes
<b>3.1.3</b> Conduct cooperative training activities, mission rehearsals, and other information exchanges to increase shared understanding of roles, responsibilities and operational capabilities (e.g., incident response teams).	Yes



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

<b>3.1.4</b> Identify potential or anticipated DHS capability and resource gaps during significant domestic cyber incident response activities to inform DoD's identification of appropriate supporting military resources.	Yes
<b>Objective 3.2</b> Support and participate in ongoing National Security Council initiatives, synchronize DHS' Emergency Cyber Action Procedures with DoD processes.	Yes
<b>3.2.1</b> Develop a standard script template for emergency Cyber Watch Conferences to ensure shared situational awareness and to facilitate planning for follow-on actions.	Yes
<b>3.2.2</b> Develop and periodically exercise standard script templates for Cyber Event Conferences, National Event Conferences, and National Threat Conferences that facilitate recommendations for Presidential or delegated representative consideration.	Yes
<b>Objective 3.4</b> Review, refine, and develop, as required, streamlined processes for formal requests for support/assistance among DHS, NSA, and USCYBERCOM.	Yes
<b>3.4.3</b> Determine and refine formal processes for NSA and USCYBERCOM to request support, as appropriate, from DHS in support of cybersecurity preparedness and incident response.	Yes
<b>Objective 3.5</b> Review as required applicable memorandums or other associated agreements between DHS, NSA, and/or USCYBERCOM and recommend changes/updates as appropriate to ensure current relevance in enhancing national cybersecurity efforts.	Yes
<b>3.5.1</b> Review the memorandum between DHS and DoD regarding Cybersecurity (signed September 2010).	Yes
<b>3.5.2</b> Review the memorandum between NSA/Central Security Service and DHS/National Protection and Programs Directorate for the establishment and Operation of a Cryptologic Support Group.	Yes
<b>3.5.3</b> Review the memorandum of DHS, NSA, and USCYBERCOM for the implementation of the Cyber Action Plan.	Yes

Source: DHS OIG analysis based on CISA testimony and evidence



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix C**  
**2018 Memorandum Lines of Effort**

<b>LOE</b>	<b>Title</b>	<b>Efforts Identified by OIG</b>
LOE 1	Intelligence, Indicators, and Warning	Yes
LOE 2	Strengthening the Resilience of National Critical Functions	Yes
LOE 3	Increasing Joint Operational Planning and Coordination	Yes
LOE 4	Incident Response	Yes
LOE 5	Integrating with State, Local, Tribal, and Territorial Governments	Yes
LOE 6	Defense of Federal Networks	Yes

Source: DHS OIG analysis based on CISA testimony and evidence



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

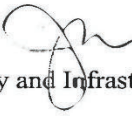
**Appendix D**  
**DHS Comments to the Draft Report**



U.S. Department of Homeland Security  
Cybersecurity & Infrastructure Security Agency  
Office of the Director  
Washington, DC 20528

September 20, 2021

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.  
Inspector General

FROM: Jen Easterly   
Director  
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "DHS Needs Additional Oversight and Documentation to Ensure Progress in Joint Cybersecurity Efforts"  
(Project No. 19-074-AUD-CISA)

Thank you for the opportunity to review and comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA is pleased to note OIG's recognition of the progress by the U.S. Department of Homeland Security (DHS or the Department) during the past 6 years to improve cybersecurity collaboration and coordination in accordance with the 2015 Cyber Action Plan (CAP) and associated memorandums.<sup>1</sup> This includes participation in critical infrastructure programs, improving cyber situational awareness, co-locating DHS and Department of Defense (DOD) liaisons, and conducting cybersecurity readiness training.

DHS remains committed to improving national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.

The draft report contained five recommendations with which the Department concurs. Attached find our detailed response to each recommendation. CISA previously submitted technical comments addressing several accuracy, contextual, sensitivity, and other issues under a separate cover for OIG's consideration.

<sup>1</sup> (1) "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," dated November 24, 2015; and (2) "Joint DoD-DHS Memorandum on the Protection and Defense of Critical Infrastructure," dated October 6, 2018.





## **OFFICE OF INSPECTOR GENERAL**

### Department of Homeland Security

---

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

### Attachment: Management Response to Recommendations Contained in OIG 19-074-AUD-CISA

OIG recommended that the Director of CISA:

**Recommendation 1:** Develop implementation plan to conduct periodic assessments for monitoring the progress of goals and activities and complete annual updates on action items as required by the Cyber Action Plan and associated 2015 and 2018 memorandums.

**Response:** Concur. CISA's Cybersecurity Division (CSD) and the DHS Office of Strategy, Policy, and Plans (PLCY) jointly represent DHS as co-chairs of the DOD-DHS Cyber Protection and Defense Steering group, as established by the "Joint DoD-DHS Memorandum on the Protection and Defense of Critical Infrastructure," dated October 6, 2018. Going forward, CISA CSD—with support from the CISA Office of Strategy, Policy, and Plans (SPP), and in coordination with DHS PLCY and DOD co-chairs—will develop an implementation plan to address the unresolved action goals, activities, and action items in the 2015 CAP, as well as the associated November 2015 and October 2018 memorandums. This effort will include conducting periodic assessments and annual updates for remaining and future goals, activities, and action items. Estimated Completion Date (ECD): March 31, 2022.

**Recommendation 2:** Conduct centralized tracking and completion of signed closeout summaries to reconcile the ongoing, outstanding, and open tasks and activities as required by the Cyber Action Plan and associated 2015 and 2018 memorandums.

**Response:** Concur. CISA CSD, with support from CISA SPP, and in coordination with DHS PLCY, will take the following steps to establish and implement a centralized tracking capability to maintain visibility and ensure progress of open action items established between DOD and DHS within the CAP and the 2015 and 2018 memorandums, as well as reconcile incomplete actions and tasks:

- CISA CSD and DHS PLCY will establish and formalize a centralized secretariat function, and supporting processes, to effectively track tasks and activities agreed upon by DOD and DHS under the 2015 CAP and the associated 2015 and 2018 memorandums.
- CISA CSD and DHS PLCY, in coordination with DOD, will conduct a thorough review of the goals, activities and action items within the 2015 CAP and associated 2015 and 2018 memorandums to identify which items remain incomplete and relevant for continued work efforts.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

- Those action items that remain incomplete and relevant for continued work efforts will be carried included in a new plan of actions and milestones (POA&M), which will be managed and tracked under the construct of the DOD-DHS Cyber Protection and Defense Steering Group, as established in the 2018 memorandum.
- Those action items that have been completed, or are no longer joint priorities, will be documented and closed-out through signed “close out summaries” that reflect the status of each action and outcomes achieved.
- Following this review of action items and development of a POA&M, CISA CSD and DHS PLCY will coordinate with DOD to formally “close out” the 2015 memorandum and CAP.

ECD: December 31, 2021.

**Recommendation 3:** Establish performance measures to ensure the effectiveness and completion of the Cyber Action Plan and associated 2015 and 2018 memorandum activities.

**Response:** Concur. CISA CSD, in coordination with DHS PLCY, will work with CISA’s Office of the Chief Financial Officer, Program Analysis & Evaluation Division to establish, and implement, performance metrics applicable to the 2015 CAP and associated 2015 and 2018 memorandum activities. Once implemented, performance metrics will be used to maintain visibility of progress and to measure effectiveness and completion. Performance metrics for active action items will be reviewed quarterly by the CISA and DHS chairs of the DOD-DHS Cyber Protection and Defense Steering Group to ensure continued visibility and to implement formal inject points for senior level guidance as needed. ECD: March 31, 2022.

**Recommendation 4:** Establish the DHS governance structure and ensure it consists of an Executive Committee that meets at least semi-annually and a Steering Committee that meets at least quarterly, as required.

**Response:** Concur. CISA CSD, with support from CISA SPP and in coordination with DHS PLCY and DOD co-chairs, will review and clarify the DHS structure under which active DOD-DHS memoranda and plans will be governed. The 2015 and 2018 memoranda prescribe different governance structures, which have not been fully reconciled. Additionally, significant reorganization has taken place within CISA and DHS since the development of the 2015 memorandum and its governance structure. Accordingly, CISA CSD and DHS PLCY will review prescribed structures and formally establish, and adhere to, a governance structure appropriate and effective for the Department given its current organizational structure. ECD: March 31, 2022.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

OIG recommended that the Under Secretary of PLCY:

**Recommendation 5:** Establish a plan, in coordination with CISA, for the appropriate allocation of technical personnel to ensure effective DHS-DoD coordination and collaboration towards cybersecurity efforts.

**Response:** Concur. In August 2020, DHS PLCY and CISA provided the DOD a prioritized request that would have fully implemented the 50-person accompaniment authorized by Section 1650 of the 2019 National Defense Authorization Act. DHS PLCY and CISA, in coordination with other operational DHS Components, will seek to reaffirm that prioritized request and will continue to work with DOD counterparts through the DOD-DHS Cyber Protection and Defense Steering Group to advocate for additional allocation of DOD technical personnel in support of joint DHS/DOD priorities. This work will continue through September 30, 2022, at which point the pilot program established under Section 1650 of the 2019 NDAA is no longer authorized. ECD: September 30, 2022.





## **OFFICE OF INSPECTOR GENERAL**

Department of Homeland Security

---

### **Appendix E**

#### **Office of Audits Major Contributors to This Report**

Tarsha Cary, Director  
Hector Daniel Urquijo, Audit Manager  
James Diaz, Program Analyst  
Jeffrey Threet, Program Analyst  
Timothy Fonseth, Program Analyst  
Zachary Israel, Auditor  
Kevin Dolloson, Communications Analyst  
John Skrmetti, Referencer



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

**Appendix F**  
**Report Distribution**

**Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chiefs of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Under Secretary, Office of Strategy, Policy, and Plans  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
Executive Assistant Director, Cybersecurity Division, CISA  
Assistant Director, National Risk Management Center, CISA  
Audit Liaison, CISA

**Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committees

## **Additional Information and Copies**

To view this and any of our other reports, please visit our website at:  
[www.oig.dhs.gov](http://www.oig.dhs.gov).

For further information or questions, please contact Office of Inspector General  
Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov).  
Follow us on Twitter at: @dhsoig.



## **OIG Hotline**

To report fraud, waste, or abuse, visit our website at [www.oig.dhs.gov](http://www.oig.dhs.gov) and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Hotline  
245 Murray Drive, SW  
Washington, DC 20528-0305