OFFICE OF INSPECTOR GENERAL

DHS Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing Attacks

Homeland Security

August 22, 2022

OIG-22-62

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 22, 2022

MEMORANDUM FOR: Eric Hysen
Chief Information Officer
Department of Homeland Security

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI Digitally signed by JOSEPH V CUFFARI Date: 2022.08.19 14:20:45 -04'00'

SUBJECT: *DHS Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing Attacks*

Attached is our final report, *DHS Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing Attacks.* We incorporated the formal comments provided by the Department.

The report contains 10 recommendations aimed at improving the Department's mitigation of risk related to malware, ransomware, and phishing attacks. The Department concurred with all 10 recommendations. Based on information provided in the Department's response to the draft report, we consider recommendations 1, 2, 3, 4, and 6 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. Recommendations 5, 7, 8, 9, and 10 are closed and resolved.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended* 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 final 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 Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing Attacks

August 22, 2022

Why We Did This Audit

Threats of cyberattacks have increased during the past two decades. We conducted this audit to determine whether DHS and its components have implemented effective controls to protect DHS' sensitive data from malware, ransomware, and phishing attacks.

What We Recommend

We made 10 recommendations to help protect DHS' information systems from malware, ransomware, and phishing attacks.

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

What We Found

In recent years, several Department of Homeland Security (DHS) components have been victims of cyberattacks. To protect its sensitive information from potential exploitation, DHS implements multiple layers of defense against malware, ransomware, and phishing attacks. DHS has also implemented specific tools and technologies to further detect and prevent security events on component systems and to help protect DHS' network communication and data.

DHS can better protect its sensitive data from potential malware, ransomware, and phishing attacks by revising its policies and procedures to incorporate new controls, in accordance with Office of Management and Budget guidance, and ensuring its users complete the required cybersecurity awareness training to mitigate risk. Further, some components did not (1) ensure all users completed required cybersecurity awareness training; (2) consistently educate users about the risks of malware, ransomware, and phishing attacks; and (3) conduct phishing exercises, as required, in fiscal years 2019 or 2020.

DHS Response

DHS concurred with all 10 recommendations. We included a copy of DHS' comments in Appendix A.

Background

Our national security and economy depend on stable, safe, and resilient information technology (IT) systems and infrastructure to carry out operations and process, maintain, and report essential information. Safeguarding sensitive data and information systems from unauthorized access and potential exploitation is a major challenge. Preventing prevalent cyberattacks, including attempts to gain unauthorized access to government information systems or sensitive data stored and processed by these systems, has been identified as one of the major management and performance challenges by the Department of Homeland Security, Government Accountability Office, and DHS Office of Inspector General.[1] Threats of cyberattacks have been increasing during the past two decades:

- According to a joint announcement from the Department of Defense (DoD), DHS, and the Department of Justice on August 3, 2020,[2] the Chinese government has been using malware[3] to target government agencies, private sector entities, and think tanks since 2008.
- The New York Times reported that, during the 2016 elections, Russian hackers used a phishing[4] attack to access about 60,000 emails in the private Gmail account of a top-ranking Democratic party official.[5]
- Days before the 2020 presidential election, phishing groups used voter registration–related lures to trick people into accessing fake government sites and giving away personal data, such as banking and email passwords and even auto registration information.[6]

In February 2022, Russia invaded Ukraine, which led to an increased public awareness of the potential for malicious cyber activity against the United States.[7] According to an April 2022 report, Microsoft observed close to 40 destructive attacks on hundreds of Ukrainian systems from February 23 to April 8, 2022, with 32 percent of these attacks directly targeting Ukrainian government organizations at various levels.[8] Actors engaging in these attacks

[1] https://www.dhs.gov/sites/default/files/2022-04/DHS%20FY21-23%20APR.pdf.
[2] https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.
[3] Malware is malicious code (e.g., viruses, worms, and bots) that disrupts service, steals sensitive information, or gains access to private computer systems, https://www.cisa.gov/report.
[4] Phishing is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques, typically via emails containing links to fraudulent websites, https://www.cisa.gov/uscert/report-phishing.
[5] https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.
[6] https://www.zdnet.com/article/phishing-groups-are-collecting-user-data-email-and-banking-passwords-via-fake-voter-registration-forms.
[7] https://www.cisa.gov/shields-up.
[8] https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

used a variety of techniques to gain initial access to their targets, including phishing, exploiting unpatched vulnerabilities, and compromising IT service providers.

In a March 21, 2022 statement, the U.S. President reiterated his warning to the Nation about the possibility of Russia conducting malicious cyber activity against the United States, including as a response to the unprecedented economic costs that we, along with our allies and partners, have imposed through sanctions on Russia.[9] To proactively address this threat, the President designated DHS as the lead Federal agency to coordinate domestic preparedness and response efforts related to the ongoing Russia–Ukraine crisis.[10]

DHS' various missions include preventing terrorism, ensuring disaster resilience, managing U.S. borders, administering immigration laws, and securing cyberspace. To accomplish this broad array of complex missions, DHS employs approximately 240,000 personnel, all of whom rely on IT to perform their duties. It is critical that DHS provide a high level of cybersecurity[11] for the information and information systems supporting day-to-day operations.

In recent years, several DHS components have also been victims of cyberattacks. In May 2019, photos of more than 100,000 travelers coming into and out of the country were stolen during an attack on a U.S. Customs and Border Protection (CBP) subcontractor's network.[12] Similarly, on October 4, 2020, United States Coast Guard (Coast Guard) personnel discovered that a database for the Coast Guard Auxiliary had been subject to a malware attack, resulting in the exfiltration[13] of contact information for 59,149 individuals who had expressed interest in joining the Coast Guard Auxiliary.

To mitigate the risks associated with malware, ransomware, and phishing attacks, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-50, *Building an Information Technology Security*

[9] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.
[10] https://www.dhs.gov/news/2022/02/24/dhs-designated-lead-federal-agency-respond-russia-related-impacts-united-states.
[11] Cybersecurity is the process of protecting information by preventing, detecting, and responding to attacks, https://csrc.nist.gov/glossary/term/cybersecurity.
[12] https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach/.
[13] Data exfiltration is a technique used by malicious actors to target, copy, and transfer sensitive data. Data exfiltration can be done remotely or manually and can be extremely difficult to detect given it often resembles business-justified (or "normal") network traffic, https://awakesecurity.com/glossary/data-exfiltration.

Awareness and Training Program,[14] October 2003, named malware and phishing as two of the nine recommended topics to be included in agencies' security awareness and training material. In addition, NIST recommends "once the program has been implemented, processes must be put in place to monitor compliance and effectiveness."

The DHS Chief Information Security Officer bears primary responsibility for protecting information and overseeing all security operations functions within the Department. Component Chief Information Security Officers establish and enforce malware protection control policies. The DHS Enterprise Security Operations Center acts as a focal point for DHS enterprise-wide cyber situational awareness. System Administrators ensure that all DHS systems use malware protection software. Information System Security Officers ensure procedures are implemented to prevent, detect, eradicate, and report malware incidents.

We conducted this audit to determine whether DHS and its components have implemented effective controls to protect DHS sensitive data from malware, ransomware, and phishing attacks.

Results of Audit

To protect its sensitive information from potential exploitation, DHS relies on multiple layers of defense against malware, ransomware, and phishing attacks, such as incident detection and prevention and network monitoring. We determined that DHS has implemented specific technologies to detect and prevent security events on component systems and to help protect DHS' network communication and data. However, DHS' policies and procedures do not reflect the latest cybersecurity standards. Also, some DHS components did not (1) ensure users completed required cybersecurity awareness training; (2) consistently educate users about the risks of malware, ransomware, and phishing attacks; and (3) conduct phishing exercises, as required, in fiscal years 2019 or 2020.[15]

[14] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf.
[15] DHS Policy Directive 034-03, *Continuous Improvement of Department of Homeland Security Cyber Defenses*, January 2016, requires components conduct phishing exercises semi-annually.

DHS Has Implemented Technologies to Prevent and Detect Cyberattacks

According to a February 2022 joint Cybersecurity Advisory statement, cybercriminals are increasingly gaining access to networks via phishing, and ransomware remains one of the most disruptive cyber threats to organizations and individuals.[16] The DHS Office of the Chief Information Officer provided a list of more than 3,000 cyber incidents the components reported between September 25, 2017, and March 13, 2021. After reviewing the list, we identified the following 115 malware, ransomware, and phishing incidents, as shown in Table 1.[17]

Table 1. Malware, Ransomware, and Phishing Incidents Reported between September 2017 and March 2021

Year	Malware	Ransomware	Phishing
2017	10	1	10
2018	55	2	5
2019	5	1	5
2020	17	1	3
2021	0	0	0
Total	**87**	**5**	**23**

Source: DHS OIG analysis

Recognizing the importance of cybersecurity, DHS has implemented several enterprise-wide tools and technologies to detect and prevent security events on component systems[18] and help protect DHS' network communication and data. For example, DHS has implemented capabilities to help monitor network traffic for potential threats and vulnerabilities, facilitate information sharing across the enterprise, and maintain an enterprise view of cybersecurity operations. Specifically, we determined that DHS:

- monitors for known cybersecurity threats, complex malware, and cyberattacks that target sensitive data;
- employs a defense in-depth cybersecurity strategy, layering security throughout the enterprise;

[16] https://www.cisa.gov/news/2022/02/09/cisa-fbi-nsa-and-international-partners-issue-advisory-ransomware-trends-2021.
[17] According to DHS personnel, the Department does not catalog unique security incidents by type (e.g., malware, ransomware, or phishing); these are generally classified as "malicious logic."
[18] The Coast Guard uses or operates networks that are connected to, or operate under, DoD information networks to support its mission.

- monitors network traffic and connections for suspicious activities; and
- deploys enterprise-wide security tools to protect component networks.

DHS also uses the following enterprise-wide detection and prevention capabilities that are managed and facilitated by the Network Operations Security Center and the Enterprise Security Operations Center:

- Detection – Detection applications identify and generate alerts for potentially malicious traffic entering or exiting the DHS enterprise network. Some applications identify malware based on predefined signatures and others monitor network traffic from known malicious domains.

- Prevention – DHS has implemented technologies with capabilities such as intrusion prevention, which automatically responds to cyber threats; firewalls that monitor, filter, and control network traffic; proxy devices that block malicious websites; and web application firewalls, which can prevent traffic from specific software or applications.

DHS' Policies and Procedures Do Not Reflect the Latest Cybersecurity Standards

NIST requires Federal agencies to establish policies and procedures to facilitate recovery from an adverse event, maintain operations, and ensure the integrity and availability of data critical to supporting operations.[19] The Office of Management and Budget (OMB) also requires[20] all legacy IT systems to meet the requirements of, and comply with, new or revised NIST standards and guidelines within 1 year of publication, unless otherwise directed by OMB.

DHS 4300A, *Sensitive Systems Handbook*,[21] provides specific techniques and procedures for implementing the requirements to protect the information that is processed by DHS' sensitive systems. For example, DHS 4300A *Sensitive Systems Handbook* requires components to:

- ensure that malware protection software is installed on every workstation, network, laptop, and mobile computing device;
- establish and enforce their own policies to protect against malware; and

[19] NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, December 2020.
[20] OMB Circular A-130, *Managing Information as a Strategic Resource,* July 2016.
[21] DHS *Sensitive Systems Handbook*, Version 12.0, November 15, 2015.

- ensure all DHS systems use malware protection software and that malware scanning occurs automatically during boot-up and installation of new software.

Although DHS has established guidance for its components to protect information and guard against cyber incidents, DHS has not updated all cybersecurity guidance. As part of this audit, we determined Attachment F of DHS 4300A, *Sensitive Systems Handbook*[22] and DHS' Concept of Operations strategy[23] did not reflect the latest cybersecurity standards put forth in NIST SPs, such as:

- NIST SP 1800-11, *Data Integrity: Recovering from Ransomware and Other Destructive Events*,[24] September 2020, describes how organizations can develop and implement appropriate actions after a detected cybersecurity event.

- NIST SP 1800-25, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*,[25] December 2020, provides a guide to help facilitate comprehensive protection from adverse events such as malware.

- NIST SP 1800-26, *Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events*,[26] December 2020, provides guidance on how organizations can develop and implement appropriate actions during a detected data integrity cybersecurity event such as destructive malware, ransomware, and malicious insider activity.

Until DHS revises its policies and procedures to reflect the latest NIST standards, the Department is less equipped to protect IT assets and cannot ensure it will be able to quickly detect, respond to, and recover from a cyberattack.

Selected Components Did Not Ensure Their Users Completed Required Cybersecurity Awareness Training

Most ransomware attacks are made possible by users who engage in unsafe practices, administrators who implement insecure configurations, or developers

[22] DHS 4300A, *Sensitive Systems Handbook, Attachment F, Incident Response*, Version 12.0, July 30, 2018.
[23] DHS *Cybersecurity Operations Concept of Operations*, Version 1.0, July 5, 2019.
[24] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-11.pdf.
[25] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-25.pdf.
[26] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-26.pdf.

who have insufficient security training.[27] With the threat of ransomware increasing, NIST recommends agencies regularly train and retrain all users to ensure they are aware of their agency's cybersecurity policies and procedures and their specific roles and responsibilities. According to NIST, it is important to train all users to use antivirus software, to install only approved software, to click only on verified links, to connect only to secured networks, and not to connect devices to public charging stations.[28]

The *Federal Information Security Modernization Act of 2014*[29] requires agencies to provide annual security awareness training to educate employees and contractors about information security risks and how to reduce these risks. NIST standards also provide security training guidance.[30] *DHS Sensitive Systems Policy Directive 4300A* requires DHS personnel to receive initial and annual refresher training on cybersecurity awareness. *DHS Enterprise Cybersecurity Awareness and Training Program Plan,* June 2017, discusses the need to standardize cybersecurity awareness training. Standardized training can reduce departmental costs and duplication of effort and ensure all DHS users receive a baseline and comprehensive level of cybersecurity education. DHS Policy Directive 034-03, *Continuous Improvement of Department of Homeland Security Cyber Defenses*, November 2017, requires components to conduct semi-annual tests, to include phishing exercises.

We determined that seven of eight DHS components evaluated did not comply with the requirements for annual cybersecurity awareness training. To determine whether staff received the required cybersecurity awareness training in fiscal years (FY) 2019 and 2020, we performed judgmental sampling to evaluate compliance for eight components.[31] After reviewing the training records, we determined that these components did not always ensure their users completed the required training. Notably, two components had less than a 50 percent completion rate for the annual cybersecurity awareness training

[27] https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf.

[28] https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf.

[29] 44 U.S.C. § 3551 *et seq.*

[30] NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, requires organizations to provide security training to system users, document and monitor information security awareness training, and retain individual training records.

[31] Components tested included U.S. Customs and Border Protection (CBP), DHS Headquarters (HQ), Federal Emergency Management Agency (FEMA), Federal Law Enforcement Training Centers (FLETC), U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), United States Coast Guard (Coast Guard), and U.S. Citizenship and Immigration Services (USCIS).

for FY 2019, and one component had less than a 60 percent completion rate for FY 2020, as shown in Table 2.

Table 2. Results of FY 2019 and FY 2020 Cybersecurity Awareness Training Records Sampled

Component	FY 2019			FY 2020		
	Total Users Sampled	Users Who Completed Training	Users Who Did Not Complete Training	Total Users Sampled	Users Who Completed Training	Users Who Did Not Complete Training
CBP	278	275	3	295	293	2
DHS HQ	229	97	132	292	284	8
FEMA	160	160	0	205	204	0
FLETC	88	40	48	93	53	40
ICE	238	235	3	278	266	12
TSA	277	270	7	285	279	6
Coast Guard	271	219	52	284	258	26
USCIS	263	258	5	293	290	3
TOTAL	**1,804**	**1,554**	**250**	**2,025**	**1,927**	**98**

Source: DHS OIG analysis

We also reviewed the cybersecurity awareness training materials from these components and evaluated the contents for consistency, according to the *Enterprise Cybersecurity Awareness and Training Program Plan*.[32] Based on our review of the training materials, we determined the components did not consistently educate users on the risks of malware, ransomware, and phishing attacks; some organizations covered these topics in more depth than others. Additionally, DHS Headquarters (HQ) did not include the topic of ransomware in its training.

We determined that only four of the eight components conducted semi-annual phishing exercises in FYs 2019 or 2020 and adequately documented the results. According to NIST, most ransomware attacks are made possible by users who engage in unsafe practices, administrators who implement unsecure configurations, or developers who have insufficient security training.[33] The Coast Guard, DHS HQ, and the Federal Law Enforcement Training Centers (FLETC) did not conduct any phishing exercises in FYs 2019 or 2020. Coast

[32] DHS *Enterprise Cybersecurity Awareness and Training Program Plan*, Version 1.0, June 7, 2017.
[33] https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf.

Guard officials stated that the component follows DoD security policy, which does not require phishing exercises. Although U.S. Immigration and Customs Enforcement (ICE) conducted semi-annual phishing exercises in FY 2020, the component did not perform any phishing exercises in FY 2019 due to contractual issues.

We also determined that the Department does not have a centralized process to track or manage cybersecurity awareness training records and that the components are responsible for implementing their own training programs. Further, component personnel cited the following reasons for why they could not provide and maintain users' cybersecurity awareness training records:

- insufficient resources and components' loss of visibility into training records data during the third quarter of FY 2019;
- technical challenges with the training platform;
- changes from one automated tracking method to another;
- manual processes used by staff to track training completion; and
- no process to validate training completed outside of training platforms (systems of record).

Standardized cybersecurity awareness training ensures all DHS users receive a comprehensive, baseline level of cybersecurity education. If users do not complete cybersecurity awareness training, DHS could be more vulnerable to malware, ransomware, and phishing attacks.

Conclusion

Safeguarding sensitive data and information systems from unauthorized access and potential exploitation has never been more important. When cyber incidents are reported quickly, DHS can use this information to render assistance and as a warning to prevent other organizations and entities from falling victim to similar attacks. However, until DHS revises its policies and procedures to reflect the latest NIST standards, the Department cannot ensure it will be able to quickly detect, respond to, and recover from a cybersecurity attack. Also, until DHS personnel are educated about the risks associated with malware, ransomware, and phishing attacks, DHS cannot ensure its sensitive information is secured.

Recommendations

Recommendation 1: We recommend the DHS Chief Information Officer (CIO) update policies and procedures to implement National Institute of Standards

and Technology standards to facilitate recovery from an adverse event and maintain operations during malware, ransomware, and phishing attacks.

Recommendation 2: We recommend the DHS CIO centrally track cybersecurity awareness training results and ensure training consistently covers malware, ransomware, and phishing.

Recommendation 3: We recommend the CBP CIO ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Recommendation 4: We recommend the DHS HQ CIO ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Recommendation 5: We recommend the FLETC CIO ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Recommendation 6: We recommend the ICE CIO ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Recommendation 7: We recommend the TSA CIO ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Recommendation 8: We recommend the Coast Guard CIO ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Recommendation 9: We recommend the DHS HQ CIO conduct phishing exercises according to the Department's requirement and document the results.

Recommendation 10: We recommend the FLETC CIO conduct phishing exercises according to the Department's requirement and document the results.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Director of the Departmental GAO-OIG Liaison Office (Director), who expressed the Department's appreciation for OIG's work planning and 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. The following is our evaluation of the Department's written comments and its response to each recommendation in the draft report.

OIG Response to Overall Management Comments

According to the Director, DHS has ongoing and planned actions to mature its Cybersecurity Awareness and Training Program, such as strengthening the Enterprise Cybersecurity Awareness and Training Program, including a new "DHS Enterprise Cybersecurity Awareness and Training Program Plan" as well as enhancing the capabilities of the Department Information Security Training Work Group. The actions described were first provide to DHS OIG in the management response dated July 28, 2022. DHS did not bring them to our attention during our audit fieldwork. Nor did DHS OCIO senior leadership raise them raised when we briefed the DHS Office of CIO (OCIO) senior leadership on our tentative findings in April 2022 or at a formal exit conference in July 2022 in which we briefed attendees on our findings. The Department also did not include any information on these actions in its technical comments to the draft report dated July 14, 2022. We look forward to receiving documentation of the Department's efforts to improve its Cybersecurity Awareness and Training Program.

Response to Report Recommendations:

The Department concurred with all 10 recommendations. Following is a summary of DHS' response to each recommendation and the OIG's analysis.

DHS Comments to Recommendation #1: Concur. DHS OCIO is updating 4300A to better align with applicable Federal mandates, DHS policy standards, and industry common practices. Once complete, this update will streamline existing policy and guidance attachments to make implementing, auditing, and updating easier. For example, the DHS Office of the Chief Information Security Officer (OCISO) is: (1) simplifying the 4300A policy process and procedures; (2) eliminating the Sensitive Systems Handbook; (3) shortening the underlying document from several hundred pages to fewer than 100 pages; and (4) socializing the updated policies with Chief Information Security Officer (CISO)

and Chief Executive Officer communities. This effort will culminate in a full update of Directive 4300A and all dependent policies by the end of FY 2022. Estimated Completion Date (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.

DHS Comments to Recommendation #2: Concur. DHS OCIO established a cybersecurity training completion reporting schedule at the start of FY 2022 in which components report completion status statistics every April and July and at the end of each fiscal year to the DHS CISO. The statistics are compiled in an executive report, which provides the DHS CIO and CISO with insight of component-level completion progress each fiscal year.

Through component CISOs, the Information Security Training Working Group also considered and provided input to DHS' Chief Human Capital Officer regarding the feasibility of implementing a single shared Learning Management System focused on cybersecurity awareness and training. DHS OCIO is currently researching the overall feasibility, potential costs, and possible cost-sharing models for future consideration in building upon this effort. ECD: September 29, 2023.

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 Comments to Recommendation #3: Concur. During FY 2020, CBP began integrating an identity management solution, which allowed for automated tracking of Cybersecurity Awareness Training completion for its 60,000+ user population. This resulted in an improvement in CBP's training compliance each year. To ensure that 100 percent of users complete initial and annual refresher security awareness training, CBP developed a report generated from the identity management solution to identify users who are non-compliant. With this report, CBP will be able to identify non-compliant users more accurately and suspend those user accounts, as well as leverage the solution's detailed audit log to investigate any anomalies. With full implementation of the report and processes by the planned completion date, CBP will ensure all users complete initial and annual refresher security awareness training, as required. ECD: October 31, 2022

OIG Analysis of DHS Comments

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

DHS Comments to Recommendation #4: Concur. In FY 2021, DHS OCIO began an initiative to significantly enhance the DHS HQ Cybersecurity Awareness and Training Program and further develop capabilities into FY 2022. For example, DHS OCIO has strengthened the annual security awareness training module, which is the required initial basic cybersecurity awareness training for new DHS "LAN-A" users. Further, DHS OCIO updated an annual cybersecurity refresher training module to include training on malware protection, phishing, and ransomware attacks. In FY 2021, DHS OCIO also established the "Cybersecurity Hot Tips Awareness Series," which consists of informative emails disseminated to all DHS HQ LAN-A network users addressing various cybersecurity topics, risks, and process/procedural instructions.

According to DHS, its leadership recognizes the importance of end user training as the first line of defense in reducing or preventing most of cyber-related attacks. Therefore, DHS OCIO is investing in a new cloud-hosted, cybersecurity-specific learning management system in FY 2022 which will provide enhanced training capability (including HQ role-based) to end users. ECD: October 31, 2022.

OIG Analysis of DHS Comments

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

DHS Comments to Recommendation #5: Concur. FLETC has policy and controls in place to address the intent of this recommendation. Specifically, FLETC Directive 140-03, *Cybersecurity Awareness, Training, and Education*, dated May 2021, requires all IT system users to complete initial cybersecurity awareness training as part of the account provisioning process and complete refresher training annually thereafter. Further, this directive requires that FLETC Information System Security Officers ensure IT system users have completed the initial cybersecurity awareness training course prior to being granted access to their assigned IT system.

Currently, the FLETC CIO uses DHS' Performance and Learning Management System to document, monitor, and retain annual refresher security awareness

training records and will maintain these processes and functions in the system DHS uses to replace PALMS. FLETC requested that the OIG consider this recommendation closed and resolved, as implemented.

OIG Analysis of DHS Comments

FLETC's actions are responsive to this recommendation. Based on the FLETC's corrective actions and the supporting documentation provided, this recommendation is closed and resolved.

DHS Comments to Recommendation #6: Concur. ICE CIO is currently improving cybersecurity awareness training, monitoring, and tracking, and is implementing the Continuous Diagnostics and Monitoring SailPoint solution to automate the account lifecycle management process. ICE CIO previously intended to integrate SailPoint with DHS' Performance and Learning Management System. Because DHS is decommissioning its Performance and Learning Management System, ICE CIO is working to ensure system integration is in place for its replacement. Once the new training platform is implemented, ICE will be able to integrate training data with SailPoint for automated alerts and account disablements. Further, ICE CIO currently conducts a manual process to achieve 100 percent compliance, which includes escalations with notifications from the user to supervisor, and account disablement for individuals who have not completed training. ECD: October 31, 2022.

OIG Analysis of DHS Comments

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

DHS Comments to Recommendation #7: Concur. The Transportation Security Administration's (TSA) current IT security awareness training ensures users of TSA information systems have general knowledge of basic principles and understand their role in the protection of TSA information and assets pursuant to the *Federal Information Security Modernization Act of 2014* (FISMA). The TSA Information Assurance and Cybersecurity Division also performs social engineering drills to educate users on the risks of malware, ransomware, and phishing attacks, and FY 2021 testing results for these activities show TSA users have success rates between 91 and 99 percent.

TSA currently uses the Online Learning Center to provide security awareness training to TSA employees and contractors. By taking this training, TSA users understand how to apply the knowledge to help secure DHS and TSA

information and information systems. As part of this training, users are also required to complete the Computer and Wireless Mobile Device Access Agreement certifying understanding of the policy and requirements for operating TSA equipment and accessing the TSA network. The Online Learning Center tracks and retains individual cybersecurity awareness training records.

TSA provides all annual security awareness training through the Online Learning Center, which can track whether users are delinquent and, if so, notify supervisors and contracting officer's representatives. The Online Learning Center then tracks delinquent users through the completion of training. According to TSA CISO, this is the best approach to ensure training requirements are met. TSA requested that the OIG consider this recommendation closed and resolved, as implemented.

OIG Analysis of DHS Comments

TSA's actions are responsive to this recommendation. Based on TSA's corrective actions and the supporting documentation provided, this recommendation is closed and resolved.

DHS Comments to Recommendation #8: Concur. On March 22, 2022, Coast Guard CIO and the Assistant Commandant for Capability released a joint ALCOAST Message to the entire Coast Guard. ALCOAST 103/22, *New Mandated Cyber Awareness Challenge* announced the launch of the newly revised Common Access Card training. The revised training features: (1) the addition of the "Controlled Unclassified Information" data category and information on handling, which replaces the "For Official Use Only" categorization; (2) telework policies/best practices and resources; and (3) Bring Your Own Devices policies/best practices, applicable to personal laptops and mobile devices.

All Coast Guard members with access to Government information systems are required to complete this annual training and digitally sign and accept the Automated Information Systems User Acknowledgement by the end of the calendar year. Failure to complete the training will result in disabling of non-compliant accounts when delinquent for more than 60 days. Coast Guard requested that the OIG consider this recommendation closed and resolved, as implemented.

OIG Analysis of DHS Comments

Coast Guard's actions are responsive to this recommendation. Based on Coast Guard's corrective actions and the supporting documentation provided, this recommendation is closed and resolved.

DHS Comments to Recommendation #9: Concur. DHS OCIO re-established phishing exercise activities and completion in FY 2022. Specifically, DHS OCIO updated the phishing metrics and activities to follow the NIST Phish Scale methodology. Further, DHS requires components to conduct a minimum of one phishing exercise per quarter, following specific metric guidelines, and report statistics to DHS CISO for oversight and statistics inclusion in the appropriate FISMA Quarterly report, as appropriate. DHS requested that the OIG consider this recommendation closed and resolved, as implemented.

OIG Analysis of DHS Comments

DHS' actions are responsive to this recommendation. Based on the Department's corrective actions and the supporting documentation provided, this recommendation is closed and resolved.

DHS Comments to Recommendation #10: Concur. FLETC CIO executed an agreement with the DHS Vulnerability Assessment Team to meet the DHS requirements to conduct annual phishing exercises and conducted its last phishing exercise on March 28, 2022. FLETC requested that the OIG consider this recommendation closed and resolved, as implemented.

OIG Analysis of DHS Comments

FLETC's actions are responsive to this recommendation. Based on the FLETC's corrective actions and the supporting documentation provided, this recommendation is closed and resolved.

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 determine whether DHS and its components have implemented effective controls to protect DHS sensitive data from malware, ransomware, and phishing attacks.

To answer our objective, we reviewed applicable policies and procedures and interviewed selected DHS personnel to determine if DHS and its components:

- established processes to monitor users' compliance and measure the effectiveness of training;
- implemented technical controls to encrypt sensitive data;
- protected sensitive data from potential exfiltration; and

- reported any security incidents in FYs 2019 and 2020, as a result of malware, ransomware, and phishing attacks.

As part of this audit, we confirmed DHS had implemented technologies to protect sensitive data. We also evaluated other controls recommended by NIST to combat ransomware, including policies, procedures, and training. Specifically, we reviewed the Department's processes, policies, and procedures pertaining to protection of sensitive data. We reviewed training requirements and records related to cyber protections from malware, ransomware, and phishing attacks.

The DHS OIG Office of Innovation's Cybersecurity Risk Assessment division provided technical support for this audit. The division reviewed technical documentation, translated technical jargon, and explained the tools and technologies DHS has implemented to protect DHS sensitive data from malware, ransomware, and phishing attacks. The division did not perform technical testing to evaluate the effectiveness of technical controls implemented.

We conducted this performance audit between December 2020 and March 2022 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 on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The Office of Audits major contributors to this report are Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division; Shawn Hatch, Supervisory IT Auditor; Sonya Davis, Auditor-in-Charge; Kate Fishler, Auditor-in-Charge; Brendan Burke, IT Auditor; Bridgette OgunMokun, Program Analyst; Samantha Stout, Program Analyst; Thomas Rohrback, Director, Office of Innovation's Cybersecurity Risk Assessment division; Jason Dominguez, Supervisory IT Cybersecurity Specialist; Rashedul Romel, Supervisory IT Cybersecurity Specialist; Taurean McKenzie, IT Specialist; Maria Romstedt, Communications Analyst; and Christine Alvarez, Independent Referencer.

Appendix A
Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

July 28, 2022

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

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER Digitally signed by JIM H CRUMPACKER Date: 2022.07.28 13:30:58 -04'00'

SUBJECT: Management Response to Draft Report: "DHS Can Better Mitigate the Risks Associated with Malware, Ransomware, and Phishing" (Project No. 21-016-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's recognition that the Department implements multiple layers of cybersecurity defense to protect against malware, ransomware, and phishing attacks, such as incident detection and prevention, and network monitoring. OIG also determined that DHS implemented technologies to detect and prevent security events on DHS Component systems and to help protect DHS's network communication and data. Leadership further notes that OIG's analysis of a sample of DHS users indicated a nine percent increase over the previous fiscal year (FY) in the completion of Cybersecurity Awareness and Training (from 86.1 percent in FY 2019 to 95.1 percent in FY 2020). DHS remains committed to protecting sensitive government information and ensuring the availability of the Department's systems to accomplish the critical mission of protecting the homeland.

However, leadership is disappointed that the OIG's findings do not provide "cold readers" of this report a more complete context regarding the actions taken, on-going, and planned to mature the Department's Cybersecurity Awareness Training Program. In FY 2021, for example, the DHS Office of the Chief Information Security Officer (OCISO) spearheaded an initiative to significantly enhance and strengthen the Enterprise Cybersecurity Awareness and Training Program, including a new "DHS Enterprise Cybersecurity Awareness and Training Program Plan"[1] and an associated work plan

[1] "DHS Enterprise Cybersecurity Awareness and Training Program Plan," Version 1.0, dated May 2022.

encompassing actions based on identified gaps within the Department and requirements specified in applicable National Institute of Standards and Technology (NIST) special publications (SP).[2]

Further, this initiative required all DHS Components to create their own Cybersecurity Awareness and Training Program Plan documenting a Component's overall training program and associated activities, in accordance with DHS Policy Directive 4300A, "Sensitive Systems Handbook," dated November 15, 2015,[3] which requires each Component to establish their own specific training program. Additionally, each Component will document annual training activities in their Cybersecurity Awareness and Training Annual Implementation Plans. All plans are scheduled to be submitted to DHS OCISO by the end of FY 2022 for review, acceptance, and oversight.

DHS OCISO also enhanced the capabilities of the Department Information Security Training Work Group (ISTWG) in FY 2022 by transitioning from a single community of interest (focused on collaboration between federal agencies) to two separate organizations. The first organization is a newly created DHS Cybersecurity Awareness Training Education and Research Community of Interest, with members from across Federal Agency Cybersecurity Awareness and Training organizations, such as DHS Components, the Department of Health and Human Services, and NIST. The second organization is a restructured ISTWG, internal to DHS, that provides recommendations for decision by the DHS Chief Information Security Officer (CISO) Council, which focuses specifically on internal DHS Cybersecurity Awareness and Training needs and actions.

Through an approved work plan, the restructured ISTWG: (1) reviewed existing DHS 4300A Cybersecurity Training policies and provided recommended updates for DHS CISO Council approval in May 2022; and (2) created role-based minimum training standards built on the NIST SP 800-181 for the initially identified roles with significant cybersecurity responsibilities. The new role-based minimum training standards were approved by the DHS CISO Council in July 2022 and implementation will begin during the remainder of FY 2022. Additional development of minimum training standards is planned through FY 2022 and future years.

The draft report contained ten recommendations with which the Department concurs. Enclosed, please find our detailed response to each recommendation. DHS previously

[2] (1) NIST 800-50, "Building an Information Technology Security Awareness and Training Program," dated October 2003; (2) NIST 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model," dated April 1998; (3) NIST 800-53, Security and Privacy Controls for Information Systems and Organizations," dated October 2020; and (4) NIST 800-181, "Workforce Framework for Cybersecurity (NICE Framework)," dated November 2020. (https://csrc.nist.gov/publications/sp)
[3] https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook.

submitted technical comments addressing any accuracy, contextual, and other issues under a separate cover for OIG's consideration.

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.

Enclosure

3

Enclosure: Management Response to Recommendations Contained in 21-016-AUD-DHS

OIG recommended that the DHS Chief Information Officer (CIO):

Recommendation 1: Update policies and procedures to implement National Institute of Standards and Technology standards to facilitate recovery from an adverse event and maintain operations during malware, ransomware, and phishing attacks.

Response: Concur. The DHS Office of the Chief Information Officer (OCIO) is currently updating 4300A to better align with applicable Federal mandates, DHS policy standards, and industry common practices. Once complete, this update will streamline existing policy and guidance attachments to make implementing, auditing, and updating easier. Specific improvements will include:

- Incorporating recently updated Federal Policies and Directives.
- Developing Organizationally Defined Values specific to DHS.
- Aligning controls with guidance provided by NIST SPs, including:
  - SP 800-53;[4]
  - SP 800-37;[5]
  - SP 800-171;[6] and
  - SP 800-161.[7]
- Modularizing policy guidance to incorporate linkages to approved Enterprise requirements, processes, standards, and guidelines.

In FY 2021, progress on this update and integration of new policies with the revision of existing policies in 4300A slowed due to a variety of exigent operational requirements. However, DHS OCISO is: (1) simplifying the 4300A policy process and procedures; (2) eliminating the Sensitive Systems Handbook; (3) shortening the underlying document from several hundred pages to fewer than 100 pages; and (4) socializing the updated policies with the CISO and Chief Executive Officer communities. This effort will culminate in a full update of DHS 4300A and all dependent policies, by the end of FY 2022.

Estimated Completion Date (ECD): September 30, 2022.

[4] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[5] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
[6] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
[7] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

4

Recommendation 2: Centrally track cybersecurity awareness training results and ensure training consistently covers malware, ransomware, and phishing.

Response: Concur. DHS OCIO established a cybersecurity training completion reporting schedule at the start of FY 2022 in which Components report completion status statistics every April and July, and at the end of each fiscal year to the DHS CISO. The statistics are compiled into an executive report which provides the DHS CIO and CISO with insight to support oversight of Component-level completion progress each fiscal year.

Through Component CISOs, the ISTWG also considered, and provided input to, the DHS Chief Human Capital Officer regarding the feasibility of implementing a single shared Learning Management System focused on cybersecurity awareness and training. DHS OCIO is currently researching the overall feasibility, potential costs, and possible cost sharing models for future consideration in building upon this effort.

ECD: September 29, 2023.

OIG recommended that the U.S. Customs and Border Protection (CBP) CIO:

Recommendation 3: Ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Response: Concur. CBP agrees with the importance of all users completing initial and annual refresher security awareness training. During FY 2020, CBP's Office of Information and Technology (OIT) began the process of integrating an identity management solution which allowed for the transition from manually tracking Cybersecurity Awareness Training completion for its 60,000+ user population to an automated process. This resulted in an improvement in CBP's training compliance each year. For example, in FY 2019, 1.07 percent of users sampled did not complete the training, and in FY 2022, completion rates improved such that only 0.6 percent of users sampled did not complete the training.

To ensure that 100 percent of users complete initial and annual refresher security awareness training, CBP OIT developed a report generated from the identity management solution to identify users who are non-compliant. With this report, CBP OIT will be able to identify non-compliant users more accurately and suspend those user accounts, as well as leverage the solution's detailed audit log to investigate any anomalies. With full implementation of the report and processes by the planned completion date, CBP will ensure all users complete initial and annual refresher security awareness training, as required.

5

ECD: October 31, 2022.

OIG recommended that the DHS CIO:

Recommendation 4: Ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Response: Concur. In FY 2021, DHS OCIO began an initiative to significantly enhance the DHS "headquarters" Cybersecurity Awareness and Training Program and further developed capabilities into FY 2022 (as documented in the DHS Cybersecurity Awareness and Training Program Plan with specific activities included in the required DHS Annual Implementation Plan). For example, DHS OCIO established, and tracks completion of, the Defense Information Systems Agency's Cybersecurity Awareness Challenge annual training module, which is the required initial basic cybersecurity awareness training for new DHS "LAN-A" network account users.

Further, in FY 2021, DHS OCIO updated an annual cybersecurity refresher training module to reflect current requirements, including training on malware protection, phishing, and ransomware attacks. In FY 2021, DHS OCIO also established the "Cybersecurity Hot Tips Awareness Series," which are informative emails disseminated to all DHS HQ LAN-A network users addressing various cybersecurity topics, risks, and process/procedural instructions to ensure appropriate end user security activities. DHS OCIO made the Hot Tips emails specifically related to malware, phishing, and ransomware available to other DHS Components for reuse in FY 2021.

Lastly, DHS OCIO significantly reengineered the cybersecurity awareness and training program and procedures in FY 2021 to ensure: (1) improved records reporting; (2) effective communications to leadership and end users on applicable requirements; and (3) an enhanced escalation reporting process for notification of non-compliant end users. In FY 2021, overall refresher training completion increased to 93 percent across the "headquarters" domain, and DHS OCIO believes that these activities will further increase overall completion.

DHS leadership recognizes the importance of end user training as the first line of defense in reducing or preventing a majority of cyber-related attacks. As such, DHS OCIO is investing in a new cloud-hosted, cybersecurity-specific learning management system in FY 2022 which will provide enhanced training capability (including "headquarters" role-based) to end users.

ECD: October 31, 2022.

6

OIG recommended that the Federal Law Enforcement Training Centers (FLETC) CIO:

Recommendation 5: Ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Response: Concur. FLETC agrees with the importance of all users completing initial and annual refresher security awareness training, and documenting and monitoring individual cybersecurity awareness training records, and notes that policy and controls are already in place to address the intent of this recommendation. Specifically, FLETC Directive 140-03, "Cybersecurity Awareness, Training, and Education" dated May 2021, requires that all IT Systems Users complete initial cybersecurity awareness training as part of the account provisioning process and refresher training annually thereafter. Further, this directive requires that FLETC Information System Security Officers ensure that IT system users have completed the initial cybersecurity awareness training course prior to being granted access to their assigned IT system.

Currently, the FLETC CIO uses the DHS Performance and Learning Management System (PALMS) to document, monitor, and retain annual refresher security awareness training records, and will maintain these processes and functions within the system that DHS uses to replace PALMS.

We request that the OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the U.S. Immigration and Customs Enforcement (ICE) CIO:

Recommendation 6: Ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Response: Concur. ICE CIO is currently in the process of improving cybersecurity awareness training, monitoring, and tracking, and is implementing the Continuous Diagnostics and Monitoring SailPoint solution to automate the account lifecycle management process. ICE CIO previously intended to integrate SailPoint with PALMS. However, as the PALMS training platform will be decommissioned, ICE CIO is working to ensure system integrations are in place for the PALMS replacement. Once the new training platform is implemented, ICE will be able to integrate training data with SailPoint for automated alerts and account disablements. Further, ICE CIO currently conducts a manual process to achieve 100% compliance, which includes escalations with notifications from the

7

user to supervisor, and account disablements for individuals who have not completed training.

ECD: October 31, 2022.

OIG recommended that the Transportation Security Administration (TSA) CIO:

Recommendation 7: Ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Response: Concur. The TSA CIO recognizes the need to ensure all users complete initial and annual refresher security awareness training, as required, and to document, monitor, and retain individual cybersecurity awareness training records. Accordingly, TSA's current IT security awareness training ensures that users of TSA information systems have general knowledge of basic principles and understand their role in the protection of TSA information and assets pursuant to the Federal Information Security Modernization Act (FISMA). TSA's Information Assurance and Cybersecurity Division (IAD) also performs social engineering drills, as required by FISMA, to educate users on the risks of malware, ransomware, and phishing attacks, and FY 2021 testing results for these activities show TSA users have success rates between 91 and 99 percent.

In addition to FISMA requirements, Section 6 (E) Policy of the TSA Management Directive No. 1400.3 "Information Technology Security," dated January 31, 2022, requires all TSA employees and contractors to "receive and complete annual information technology security awareness and privileged user training, when applicable."

Currently, TSA IAD utilizes the Online Learning Center (OLC) to provide security awareness training to TSA employees and contractors. By taking this training, TSA users understand how to apply the knowledge to help secure DHS and TSA information and information systems, including such subjects as: (1) information security policy and governance; (2) data security; (3) cyber safety while teleworking, including the risks of malware, ransomware and phishing attacks; and (4) requirements when requesting or purchasing software. As part of this training, users are also required to complete the Computer and Wireless Mobile Device Access Agreement certifying understanding of the policy and requirements for operating TSA equipment and accessing the TSA network. OLC tracks and retains individual cybersecurity awareness training records.

Refresher or remedial training is also required for individuals who have been determined, through FISMA IT security awareness training or other indicators, to need additional training. Training and the record of the completion of training is also tracked in OLC. Further, as all annual security awareness training is provided and tracked through OLC when users are delinquent, supervisors and Contracting Officer Representatives are

8

notified by the system, and OLC then tracks users through to the completion of the training with continued delinquency reports. TSA CISO believes that this is the best approach to ensure training requirements are met, as TSA is generally above 97 percent for security awareness training completion, which was previously provided to OIG under a separate cover.[8] In particular, for one data call, TSA provided documentation that 67,459 employees had completed the training, and a sampling of these employees who had completed training in 2019 and 2020, which demonstrated TSA achieved a 97 percent rate of completion in both years.

We request that the OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the U.S. Coast Guard (USCG) CIO:

Recommendation 8: Ensure all users complete initial and annual refresher security awareness training as required and document, monitor, and retain individual cybersecurity awareness training records.

Response: Concur. On March 22, 2022, the Coast Guard Chief Information Officer and Assistant Commandant for Capability released a joint ALCOAST Message to the entire Coast Guard, ALCOAST 103/22, "New Mandated Cyber Awareness Challenge," which announced the launch of the newly revised Common Access Card training. The revised training features: (1) the addition of the "Controlled Unclassified Information" data category and information on handling, which replaces the "For Official Use Only" categorization; (2) telework policies/best practices and resources; and (3) Bring Your Own Devices policies/best practices, applicable to personal laptops and mobile devices.

All Coast Guard members with access to government information systems, including Active Duty, Reserves, Civilians, Auxiliarists, Contractors, Non-Appropriated Funds Employees, and Ombudsmen, are required to complete this annual training and digitally sign and accept the Automated Information Systems User Acknowledgement by the end of the calendar year. Failure to complete the training will result in disabling of non-compliant accounts when delinquent for more than 60 days.

We request that the OIG consider this recommendation resolved and closed, as implemented.

[8] TSA's FY 2019 and FY 2020 security awareness training data were provided to the OIG in June 2021. The FY22 data were provided in June 2022.

OIG recommended that the DHS CIO:

Recommendation 9: Conduct phishing exercises according to the Department's requirement and document the results.

Response: Concur. DHS OCIO re-established phishing exercise activities and completion in FY 2022 by requiring each Component to conduct phishing exercises in the "FY 2022 Information Security Performance Plan" (ISPP), Version 5.0, dated January 18, 2022, in order to rebaseline and capture training metrics related to the overall DHS Information Technology user's ability to recognize various forms and strengths of phishing attacks. Specifically, DHS OCIO updated the phishing metrics and activities to follow the NIST Phish Scale methodology.[9] Further, the ISPP requires Components to conduct a minimum of one phishing exercise per quarter, following specific metric guidelines, and report statistics to the DHS CISO for oversight and statistics inclusion in the appropriate FISMA Quarterly report,[10] as appropriate.

We request that the OIG consider this recommendation resolved and closed, as implemented.

OIG recommended that the FLETC CIO:

Recommendation 10: Conduct phishing exercises according to the Department's requirement and document the results.

Response: Concur. The FLETC CIO executed an agreement with the DHS Vulnerability Assessment Team to meet the DHS requirements to conduct annual phishing exercises and conducted its last phishing exercise on March 28, 2022.

We request that the OIG consider this recommendation resolved and closed, as implemented.

[9] https://www.nist.gov/publications/nist-phish-scale-method-rating-human-phishing-detection-difficulty
[10] https://www.cisa.gov/federal-information-security-modernization-act

Appendix B
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
Chief Information Officer
Chief Information Security Officer
Audit Liaison, Office of the Chief Information Officer
Audit Liaison, Office of the Chief Information Security Officer
Audit Liaisons, CBP, FEMA, FLETC, ICE, TSA, Coast Guard, and USCIS

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.

For further information or questions, please contact Office of Inspector General Public Affairs at: 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 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