U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-40 July 17, 2024

FINAL MANAGEMENT ALERT

Management Alert - CISA and FLETC Did Not Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curricula

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

July 17, 2024

MEMORANDUM FOR: Robert Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency

Michael L. Vesta
Chief Information Officer
Federal Law Enforcement Training Centers

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.07.17 06:59:56 -07'00'

SUBJECT: *Management Alert – CISA and FLETC Did Not Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curricula*

Attached is our final management alert, *CISA and FLETC Did Not Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curricula*. This alert informs you of urgent cybersecurity issues we discovered during an ongoing audit, and the actions the components have taken to address the issues. Specifically, we found CISA and FLETC did not take action to protect personally identifiable information and sensitive law enforcement training curricula.

Your office concurred with our recommendations in the draft management alert. Based on information in your office's response to the draft management alert, we consider the two recommendations open and resolved. As appropriate, we incorporated your technical comments. We have appended your office's response verbatim to this final management alert.

As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes, for each recommendation, any update to your concurrence or nonconcurrence and any planned corrective action with a targeted completion date or completed corrective action. Also, please include information on responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act of 1978*, we will provide copies of our alert to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the alert on our website for public dissemination.

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

Attachment

Summary of Issues

During our ongoing audit of the Department of Homeland Security's learning management system (DHSLearning), we identified a significant risk to the operations, assets, and individuals at the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Law Enforcement Training Centers (FLETC). We are issuing this management alert to advise CISA and FLETC to take immediate action to mitigate risks associated with using a high-risk contractor (Contractor A) to supply their learning management systems. A DHS internal investigation identified Contractor A as having poor cybersecurity practices. By not taking action to mitigate the control deficiencies, CISA and FLETC may be putting sensitive personally identifiable information (PII) and sensitive law enforcement training information stored and processed by CISA and FLETC's learning management systems at risk of compromise.

Background

DHS and its components use learning management systems to provide online training to personnel and stakeholders. In August 2022, DHS entered into an interagency agreement with the Office of Personnel Management to use Contractor A to acquire a learning management system software as a service solution to meet enterprise training needs. Software as a service works through a cloud delivery model in which a contractor hosts applications and data on its servers and databases. The service contractor is responsible for the operation, management, and continuous monitoring in accordance with security controls.

On May 27, 2023, 7 months after the Department launched DHSLearning, the system experienced multiple hard drive failures. The incident caused a service outage and loss of DHS data. Specifically, DHS' learning management system went offline for 6 days. Despite remote and on-site attempts, hardware resets, and installation of new replacement drives, the data could not be recovered because no system backups were being performed due to an incorrect configuration. Following the incident, an investigation by the DHS Chief Information Security Officer (CISO) concluded Contractor A had poor cybersecurity practices and was not complying with Federal Risk and Authorization Management Program (FedRAMP) monitoring requirements.[1] The investigation found Contractor A:

- did not actively monitor its data center or hardware health alerts;
- utilized hardware at the end of its useful life;

[1] FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud technologies across the Federal Government. The FedRAMP Program Management Office resides within the U.S. General Services Administration. It supports agencies and cloud service providers through the FedRAMP authorization process and maintains a secure repository of FedRAMP authorizations to enable reuse of security packages.

- performed hundreds of datastore snapshots of the system on the evening prior to the outage, yet logs did not show similar snapshots in the months preceding the hard drive failure;
- shared use of administrative accounts that cannot be attributed to any one privileged user;
- failed to meet log-retention and audit logging requirements; and
- released Federal data to a third-party recovery service without authorization.

As a result of the investigation, the DHS CISO determined that continued use of DHSLearning posed an unacceptable risk to DHS operations, assets, and individuals. On June 23, 2023, the DHS CISO issued a denial of the authorization to operate (ATO) and ordered all employees to stop using DHSLearning because it could not rule out the possibility of a malicious insider or cyberattack.

According to *DHS Sensitive Systems Policy Directive 4300A*, a denial of authorization means that the information system is not authorized to operate and that there are significant deficiencies in the system's controls. If the system is currently in operation when a denial is issued, all system activity must be halted. Having an approved ATO is critical because it demonstrates that a Federal agency has gone through a federally approved, detailed process to protect an information technology system from incidents such as cyberattacks, security breaches, malware, and phishing attempts.

On July 21, 2023, the DHS CISO notified all component CISOs about the denial and shared the results of the investigation since both CISA and FLETC also use Contractor A to supply their learning management systems. CISA's learning management system, Federal Virtual Training Environment (FedVTE), is a free, online, and on-demand cybersecurity training system that is widely available to U.S. Government personnel (Federal, military, state, local, tribal, and territorial government) and veterans. FedVTE is a privacy-sensitive system that collects names and email addresses from approximately 500,000 users nationwide. Examples of training courses include:

- Mobile and Device Security;
- Preventing Web and Email Server Attacks;
- Securing Infrastructure Devices; and
- Defend Against Ransomware Attacks.

FLETC's learning management system, eFLETC, is an online learning management environment supporting law enforcement training for Federal, state, local, tribal, and international law enforcement officers. According to its June 2017 Privacy Impact Assessment, FLETC's system collects, maintains, uses, and disseminates PII from 37,591 DHS and other Federal law enforcement officers who are registered users of the system. It collects information such as

name, social security number, date of birth, gender, rank, and title. It also includes sensitive law enforcement training topics, such as:

- Active Shooter Threat;
- Protective Detail Refresher;
- Seaport Security Anti-Terrorism;
- Law Enforcement Control Tactics Refresher;
- Handgun Optic; and
- Covert Electronics.

CISA and FLETC Did Not Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curricula

On June 23, 2023, the same day the DHS CISO issued the denial of authorization for DHSLearning, CISA's Chief Information Officer (CIO) rescinded the ATO for FedVTE. However, 3 days later, CISA's CIO signed a Risk Acceptance memorandum authorizing the continued use of FedVTE even though it identified the overall risk to CISA's operation as "high due to anomalies found during DHS' investigation." CISA's CIO recommended "accepting the risk to allow the learning management system to continue operating given its impact across the Federal, state, local, and private industry mission space, until CISA can develop a new capability, transition to another capability, or the FedRAMP provider brings the system to an acceptable level of compliance with DHS and CISA standards."

CISA's Risk Acceptance request did not comply with DHS 4300A Attachment B,[2] which requires the request to include:

- the weaknesses identified;
- justification for the request;
- any compensating controls;
- a Plan of Action and Milestones, which includes the specific tasks needed to correct the deficiencies;
- the resources required to accomplish the tasks;
- scheduled completion dates; and
- approval by the DHS CISO.

We found that CISA's Risk Acceptance request did not include a valid justification, compensating controls, or a Plan of Action and Milestones to remediate the identified control deficiencies and

[2] DHS 4300A, *Information Technology System Security Program, Sensitive Systems,* Attachment B, *Information System Waiver and Risk Acceptance Requests*, July 2022.

protect its learning management system from cybersecurity vulnerabilities. Additionally, CISA's CIO both authored and approved its Risk Acceptance request without any oversight or approval from the DHS CISO, as required. As of July 2024, CISA had not developed a new capability, transitioned to another capability, or taken any steps to ensure Contractor A complies with DHS and CISA standards.

FLETC also continued using eFLETC after being notified of the denial of authorization by the DHS CISO. In FLETC's original ATO for eFLETC (issued June 9, 2022), the FLETC CIO certified that the system met the necessary security requirements but noted that the ATO would only remain valid if the Contractor A maintained compliance with FedRAMP's continuous monitoring requirements. Even though DHS' investigation found noncompliance by Contractor A with FedRAMP's monitoring requirements, FLETC did not rescind its ATO or take any steps to mitigate these risks. Instead, 1 month after being notified of the investigation results, FLETC signed a 1-year, $1.8 million extension to continue using Contractor A for eFLETC.

By not mitigating new risks to its operations, assets, and individuals, DHS cannot be assured that effective controls are in place to protect sensitive information stored and processed by CISA and FLETC's learning management systems. According FLETC's Privacy Impact Assessment, eFLETC collects, maintains, uses, and disseminates PII about all law enforcement officers, such as name, social security number, date of birth, gender, rank, and title. CISA's FedVTE is also a privacy-sensitive system for members of the public, DHS personnel, and other Federal employees. Until DHS ensures that Contractor A complies with DHS security standards, CISA and FLETC will continue to put users' PII at risk and expose sensitive courses housed on the systems.

Recommendations

Recommendation 1: We recommend the CISA Chief Information Officer immediately mitigate the control deficiencies or cease operation of the Federal Virtual Training Environment system.

Recommendation 2: We recommend the FLETC Chief Information Officer immediately mitigate the control deficiencies or cease operation of the eFLETC system.

Management Comments and OIG Analysis

CISA and FLETC concurred with our recommendations. Appendix B contains a copy of CISA and FLETC's response in its entirety. We also received technical comments and revised the report as appropriate. We consider both recommendations open and resolved. A summary of CISA's and FLETC's response to the recommendations and our analysis follows.

CISA's Response to Recommendation 1: Concur. CISA's Office of the Chief Information Officer is working to replace FedVTE with another service solution to meet training needs, with an initial

operating capability scheduled for delivery by September 30, 2024. In the interim, CISA is establishing processes to immediately mitigate control deficiencies. Estimated Completion Date: December 31, 2024.

OIG Analysis of CISA's Response: These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when CISA provides its formal document replacing FedVTE with another service solution to meet training needs.

FLETC's Response to Recommendation 2: Concur. FLETC's eLearning and Training Analytics Division is actively pursuing a replacement for the eFLETC learning management system, with an estimated transition by April 30, 2025. In the interim, FLETC set processes to immediately mitigate control deficiencies such as periodically backing up its data independently from the vendor. Estimated Completion Date: June 30, 2025.

OIG Analysis of FLETC's Response: These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when FLETC provides documentation of its periodic backups, mitigating measures for the vendor's noncompliance of audit logging and retention requirements, or evidence it has replaced the eFLETC learning management system.

Appendix A
Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107−296) by amendment to the *Inspector General Act of 1978*.

We issued this management alert as part of an ongoing audit of DHS's acquisition of a learning management system. The objective of our ongoing audit is to determine to what extent DHS defined and tested requirements in accordance with Federal and departmental policy prior to procuring a learning management system to support its training needs.

As part of our audit, from October 2023 to March 2024, we interviewed officials from DHS, CISA, and FLETC. We obtained and analyzed relevant documents relating to the learning management systems. We also reviewed:

- *DHS Sensitive Systems Policy Directive 4300A* and Attachments;
- *DHS System Security Authorization Process Guide, Version 14.1*; and
- *NIST Special Publication 800-37 Revision 2*.

We conducted this work pursuant to the *Inspector General Act of 1978,* 5 U.S.C. §§ 401-424, and in connection with an ongoing audit being performed according to generally accepted government auditing standards. Those standards require we plan and perform our audit work to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. Additional information and recommendations related to the issues addressed in this management alert may be included in the report resulting from our audit.

DHS OIG's Access to DHS Information

During this audit, DHS provided timely responses to our requests for information and did not delay or deny access to information we requested.

Appendix B:
DHS Comments on the Draft Alert

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

Homeland Security

July 3, 2024

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

FROM: On behalf of:
Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office
DAVID E SCHMITT Digitally signed by DAVID E SCHMITT Date: 2024.07.03 14:39:53 -04'00'

SUBJECT: Management Response to Draft Report: "Management Alert – CISA and FLETC Did Note Take Action to Protect Personally Identifiable Information and Sensitive Law Enforcement Training Curriculum"
(Project No. 23-045-AUD-DHS(a))

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.

As OIG recognized, on June 23, 2023, the DHS Office of the Chief Information Officer (OCIO), Chief Information Security Officer Directorate (CISOD) issued a denial of the authorization to operate the "DHS Federal Learning Enclave (DHS FLE)" based on the outcome of an internal cybersecurity investigation. This denial of authorization to operate included the DHS Learning Management System (DHS Learning) Software as a Service (SaaS) procured through an interagency agreement with the Office of Personnel Management (OPM).

Specifically, on May 27, 2023, DHS OCIO CISOD was alerted to a potential cybersecurity incident involving a system failure of the DHS FLE, which caused the DHS Learning SaaS to go offline and resulted in loss of DHS data. DHS OCIO CISOD promptly investigated, and concluded that, despite significant time and effort committed to partnering with OPM in its incident response efforts, DHS OCIO CISOD could not rule out the possibility that a malicious insider or external cyber attacker either caused or was a contributing factor in the DHS Learning system outage.

DHS OCIO CISOD shared the results of the investigation and its denial of authorization to operate with all Components, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Law Enforcement Training Centers (FLETC). DHS leadership takes seriously all concerns of risks to its systems and information, including sensitive personally identifiable information (PII) and sensitive law enforcement training information. CISA and FLETC have taken action proactively to replace their Component learning management systems as quickly as possible.

DHS and its Components remain committed to ensuring that IT service contractors maintain high-quality operation, management, and continuous monitoring in accordance with security controls, as appropriate.

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

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.

Enclosure

Enclosure: Management Response to Recommendations Contained in OIG (23-045-AUD-DHS(a))

OIG recommended the CISA Chief Information Officer (CIO):

Recommendation 1: Immediately mitigate the control deficiencies or cease operation of FedVTE [Federal Virtual Training Environment] system.

Response: Concur. The CISA Office of the Chief Information Officer (OCIO) is working to replace FedVTE with another service solution to meet training needs, with an initial operating capability scheduled for delivery by September 30, 2024. In the interim, CISA OCIO set in place, or is establishing the following processes, to immediately mitigate control deficiencies:

- On October 1, 2023, CISA established a "Security Operations Center and Technical Operations Center" to provide continuous monitoring of CISA systems by providing near-real-time active security compliance information to CISA OCIO for situational awareness. Accordingly, CISA does not have to wait a month to receive compliance information from FEDRAMP/Cloud Service Providers, which makes CISA's security monitoring much more effective and accurate.
- CISA OCIO currently conducts monthly reviews of the OPM FEDVTE Federal Risk and Authorization Management Program (FEDRAMP)[1] system scan compliance report, which is a government-wide compliance program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. CISA's monthly reviews helps ensure that any high or critical findings are elevated to the CISA Deputy CISO within 24 hours. The most recent review in June 2024 did not identify any high, or critical risks, to the system, and
- CISA will complete a standard operating procedure addressing "risk acceptance memoranda" by July 31, 2024, to ensure CISA is fully compliant with DHS Sensitive Systems Policy Directives and related attachments.[2]

Estimated Completion Date (ECD): December 31, 2024.

[1] FedRAMP is a governmentwide program, managed by the U.S. General Services Administration, which provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. For more information, see https://www.gsa.gov/technology/government-it-initiatives/fedramp.
[2] See DHS Policy Directive 4300A, "Information Technology System Security Program, Sensitive Systems," Version 13.3, dated February 13, 2023 found https://www.dhs.gov/sites/default/files/2023-05/V2.508%20Working%20file_DHS_4300A%20ITSSP%20SS%20Policy%20Directive%20FINAL%202023.02.13_kwb.pdf. See also DHS Directive 4300A Attachment B, "Information System Waiver and Risk Acceptance Requests," Version 1.0, dated July 30, 2022 found https://www.dhs.gov/sites/default/files/2023-06/4300A%20ITSSP%20SS%20Attachment%20B%20Waiver%20and%20Risk%20Acceptance%20Request%20Form.pdf.

OIG recommended the FLETC CIO:

Recommendation 2: Immediately mitigate the control deficiencies or cease operation of eFLETC [FLETC's eLearning and Training] system.

Response: Concur. FLETC's eLearning and Training Analytics Division is actively pursuing a replacement for its eFLETC learning management system with an estimated transition to this new system by April 30, 2025. In the interim, FLETC set in place the following processes to immediately mitigate control deficiencies:

- Since September 2019, the current eFLETC learning management system is provided to FLETC under its own interagency agreement with OPM separate from the DHS Learning SaaS;
- The draft report's reference to FLETC's June 21, 2017, Privacy Impact Assessment for eFLETC does not reflect current data collection practices. Specifically, on June 24, 2024, the DHS Privacy Office reviewed and adjudicated a Privacy Threshold Analysis for eFLETC, which stated that eFLETC does not collect, maintain, use, or disseminate Social Security numbers or other types of stand-alone sensitive PII. Accordingly, the FLETC Privacy Office is working with the DHS Privacy Office regarding an update to the Privacy Impact Assessment for eFLETC.
- Beginning July 2023, FLETC's eLearning and Training Analytics Division periodically backs up its data independently from the vendor; and
- On February 2, 2024, FLETC's Cyber Security Division completed an assessment of the vendor's compliance with enhanced audit logging and retention requirements and found the vendor to be non-compliant. Accordingly, FLETC's Cyber Security Division is working with contracting and program officials at the OPM to ensure the contractor complies with the enhanced audit logging and retention requirements detailed in Office of Management and Budget Manual M-21-31[3] by September 1, 2024.

ECD: June 30, 2025.

[3] "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," dated August 27, 2021; https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

4

Appendix C:
Alert 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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov

DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

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