~~LAW ENFORCEMENT SENSITIVE~~

U.S. DEPARTMENT OF HOMELAND SECURITY
OFFICE OF INSPECTOR GENERAL

OIG-24-02 October 30, 2023

FINAL MANAGEMENT ALERT

Management Alert - ICE Management and Oversight of Mobile Applications (REDACTED)

~~LAW ENFORCEMENT SENSITIVE~~

~~*WARNING: This document is Law Enforcement Sensitive (LES). Do not distribute or copy this report without the expressed written consent of the Office of Inspector General.*~~

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

October 30, 2023

MEMORANDUM FOR: Patrick J. Lechleitner
Deputy Director and Senior Official Performing the Duties of the Director
U.S. Immigration and Customs Enforcement

The Honorable 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: 2023.10.27 16:25:39 -07'00'

SUBJECT: Management Alert – *ICE Management and Oversight of Mobile Applications* ~~– Law Enforcement Sensitive / For Official Use Only~~

Attached is our final management alert, *ICE Management and Oversight of Mobile Applications* – ~~Law Enforcement Sensitive / For Official Use Only~~. This alert informs you of urgent issues we discovered during an ongoing audit and the actions ICE and DHS have taken to address the issues. Specifically, we found mobile device management issues that put ICE mobile devices — and potentially other DHS mobile devices demonstrating similar issues — and sensitive data at greater risk of potential espionage, leaks, and attacks from viruses.

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

OIG Project No. 23-017-AUD-ICE (a)

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, with appropriate redactions, on our website for public dissemination.

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

Attachment

Summary of Issues

During our ongoing audit to determine the extent to which U.S. Immigration and Customs Enforcement (ICE) manages and secures its mobile devices, we identified thousands of mobile applications installed by ICE employees, contractors, and other DHS agency[1] employees on ICE-managed mobile devices. These included applications from companies banned from U.S. Government information systems, applications associated with [redacted] and [redacted], third-party file sharing applications, third-party virtual private networks (VPN), and outdated messaging applications.

These user-installed mobile applications pose a risk to ICE's operations, its employees, and the Department. Among other things, these applications introduce the potential for collecting and monitoring user and device information through device sensors such as a camera, microphone, and Global Positioning System. The applications may also collect and distribute information stored on the device (e.g., photos, videos, and documents), including potentially sensitive information outside the secure containers. This risk is intensified given that some of the mobile applications identified are associated with U.S. Government foreign adversaries.

These risky user-installed mobile applications were present on ICE devices due to ICE's outdated and overly permissive personal use policy,[2] which enables nearly unlimited personal use of ICE-issued mobile devices. Additionally, ICE did not sufficiently manage, monitor, or assess most user-installed applications for potential impacts on device or data security because ICE considered them to be personal applications. Finally, although ICE implements certain security controls, those controls did not sufficiently reduce the risk to ICE mobile devices and their sensitive information.

Background

ICE promotes homeland security and public safety through the criminal and civil enforcement of Federal laws governing border control, customs, trade, and immigration. To assist in carrying out their duties, ICE personnel and contractors are provided ICE-issued mobile devices (e.g., smartphones) that provide telecommunication, connectivity to ICE information systems, and work-related applications. For example, one ICE-owned application allows ICE personnel to capture and search biometric information of people they encounter in real-time. In addition to work-related applications, ICE allows personnel (i.e., mobile device users) to install mobile

[1] In April 2023, ICE's Office of the Chief Information Officer (OCIO) managed about [redacted] mobile devices for other DHS agencies within its Mobile Device Management (MDM) system. As a result, some of the risky applications identified could reside in mobile devices owned by the Federal Protective Service and the Office of Biometric Identity Management.

[2] ICE Policy Number 4004.1, *Use of ICE-Issued Mobile Devices*.

applications directly from third-party application stores. These "user-installed" applications include text messaging applications used for official business, as well as applications related to maps, weather, and airlines for personal convenience.

DHS components must follow DHS' information security policies, which are integrated with National Institute of Standards and Technology (NIST) security publications. According to NIST mobile device guidance, organizations should plan their mobile device security with the assumption that unknown third-party mobile device applications downloadable by users should not be trusted.[3] The guidance further states that any application installed on a mobile device can act as a portal for the developer to compromise the device and access sensitive enterprise information. DHS' mobile device policy requires components to centrally manage approved mobile applications, allowing for application vetting, monitoring of installed applications, and upgrading or uninstalling applications remotely, as necessary. The policy also requires components to disable and remove any unapproved or unnecessary mobile device applications whenever possible.[4]

The DHS Chief Information Security Officer (CISO) is responsible for strengthening the Department's information security program; and ICE's CISO oversees the security of ICE's networks, user access, and ensures ICE complies with information security requirements. ICE's OCIO is responsible for establishing ICE's security standards of mobile devices, as well as providing administrative support, operations, and device monitoring.

Risky Applications Were Installed on ICE-Managed Mobile Devices

We identified numerous risky user-installed mobile applications on ICE-managed mobile devices. Among the approximately [redacted] mobile applications installed[5] on about [redacted] mobile devices as of April 2023, we identified:

- Applications from companies banned from U.S. Government information systems due to spying and national security risks;
- Applications associated with [redacted] and [redacted];
- Third-party file sharing applications;
- Third-party VPNs; and
- Third-party messaging applications, some with known vulnerabilities.

[3] NIST Special Publication 800-124 Revision 2, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* May 2023.

[4] DHS Policy Directive 4300A Attachment I, *Sensitive Mobile Devices*.

[5] Over [redacted] unique applications were installed on mobile devices. Each application had one or more versions, leading to a total of over [redacted] applications installed.

Banned Company Applications

We identified [redacted] applications installed from companies banned by U.S. law, Cybersecurity and Infrastructure Security Agency (CISA) directives, or the ICE Security Operations Center (SOC). [redacted]

Equipment, software, and services from certain companies are legally banned from U.S. Government systems.[6] According to U.S. law, these applications and devices pose a risk of spying or disrupting U.S. communications and are an unacceptable risk to national security.[7] Similarly, CISA Binding Operational Directives and the ICE SOC also list equipment and software applications that should not be on ICE systems.

Applications Associated with [redacted] and [redacted]

We identified [redacted] [redacted] and [redacted] [redacted] applications installed on ICE mobile devices that use internet domains from both [redacted] and [redacted] These applications posed a risk to ICE data, as companies managing such software may be compelled to provide data to foreign governments. For example, we found a [redacted] cloud storage application whose company's Chief Executive Officer is sanctioned by the U.S. Department of Treasury. [redacted] assistance from [redacted] companies to intercept communications through [redacted] networks.

We also found an application developed by [redacted] This application was designed to obtain device location, access photos, create video recordings, retrieve information about current or recently run applications, read contacts, obtain other device information, and change system settings. The application may also share information with third parties, including companies banned by the *National Defense Authorization Act,* Section 889. In addition, the application could share information with the government of [redacted] subject to [redacted] law. [redacted]

CISA describes the cybersecurity threats posed by [redacted] and [redacted] as advanced and persistent. The [redacted] government engages in malicious cyber activities including cyber espionage, theft of intellectual property, and other cyber activities meant to harm its adversaries. [redacted] likely

[6] *Secure and Trusted Communications Networks Act of 2019*, Pub. L. No. 116-124; *National Defense Authorization Act for Fiscal Year 2019*, Pub. L. No. 115-232.
[7] *Id.*

represents the broadest, most active, and persistent cyber espionage threat to the U.S. Government.

Third-Party File Sharing and Cloud Services

We identified more than [redacted] file sharing, photo sharing, and cloud service applications on ICE mobile devices. When cloud-based systems are under the organization's control, risk is generally acceptable, but connecting an organization-issued mobile device to a third-party file sharing site, such as a remote photo backup service, may place the organization's data at risk of being stored in an unsecured location outside of the organization's control. In addition, unauthorized cloud services are prohibited by DHS because they could spread viruses.

Third-Party VPNs

We identified the existence of at least [redacted] third-party VPNs. The more widely installed VPNs used servers located in several foreign countries around the world.

In a 2019 response to a congressional inquiry regarding the existence of foreign VPNs on Federal employees' Government-issued phones, the CISA Director stated, "Even with the implementation of technical solutions, if a U.S. Government employee downloaded a foreign VPN application originating from an adversary nation, foreign exploitation of that data would be somewhat or highly likely. This exploitation could lead to loss of data integrity and confidentiality of communications transmitted over the application. Exposure of data would likely include contacts, user history, geolocation, photographs, and any other accesses granted by the user to the application."[8]

Therefore, it is extremely concerning that two of the third-party VPNs we identified were [redacted], one of which was developed by a company with close ties to [redacted]

Third-Party Messaging Applications

Although discouraged by ICE's OCIO due to records retention concerns, ICE employees can use third-party text messaging applications for official business when needed. However, nearly [redacted] third-party messaging applications were installed on ICE mobile devices.

We assessed the most widely used third-party messaging applications and identified high and critical known vulnerabilities[9] on versions installed on [redacted] devices. They included weaknesses that could have resulted in the corruption of data, remote code execution, or allowed an attacker to send devices a legitimate-looking link that would direct users to malicious sites. Since ICE

[8] Christopher C. Krebs, letter to the Honorable Ron Wyden, 22 May 2019.
[9] Published in the NIST's National Vulnerability Database.

employees use these applications for official business, it is particularly important that they are securely managed. However, the most widely downloaded third-party messenger was out of date for more than a month on [redacted] of devices, which can make these devices more vulnerable. We also identified several hundred installations of other third-party messaging applications that self-delete messages and enable anonymous messaging.

Factors Leading to Risky Applications on ICE-Managed Mobile Devices

These risky user-installed mobile applications were present on ICE devices due to ICE's outdated and overly permissive personal use policy. Additionally, ICE did not sufficiently manage, monitor, or assess most user-installed applications for potential impacts on device or data security. Finally, although ICE implemented certain security controls, those controls did not sufficiently reduce the risk associated with these applications.

ICE Personal Use Policy for Government-Issued Devices

Last updated in 2014, ICE's personal use policy allows for nearly unlimited personal use of ICE-issued mobile devices.[10] For example, the policy permits ICE employees and contractors to:

- download applications and stream digital media;
- use social media and personal shopping sites;
- use internet-based phone services;
- use personal email; and
- send and receive personal messages.

Some of the approved uses were not consistent with current DHS personal use policy,[11] which prohibits the use of information systems for personal internet activities such as streaming audio or video, social networking, personal email, and unauthorized instant messaging.

ICE Did Not Sufficiently Manage, Monitor, or Assess Mobile Applications

User-installed applications were considered personal, and ICE did not require staff to extensively monitor the applications downloaded by ICE employees and contractors. ICE allowed users to install nearly any application available through commercial mobile application stores except for [redacted] applications blocklisted by the ICE SOC. Blocklisted applications included [redacted]

[10] ICE prohibits viewing, storing, and transmitting sexually explicit or predominately sexually oriented material, as well as activities related to gambling, illegal weapons, terrorist activity, or any other activity prohibited by law or agency policy.

[11] DHS Policy Directive 4300A Attachment G, *Rules of Behavior*.

NIST recommends organizations employ a vetting process to ensure a level of confidence that applications are free from vulnerabilities.[12] In addition to blocklisting, NIST describes allowlisting, which allows users to only install applications that have been preauthorized. ICE has not implemented allowlisting, although DHS policy identifies allowlisting as a control.[13]

Mitigating Controls Were Not Sufficient

DHS Management officials believed existing controls sufficiently mitigated the risks associated with the user-installed applications. These controls included secure software containers, MDM, and Mobile Threat Defense software. We determined that these controls did not sufficiently reduce these risks.

- Secure Containers: Secure containers are intended to provide software-based data isolation designed to segment enterprise applications and information from user-installed applications and data. However, ICE devices may hold photographic evidence, geographic location data, call history, text messages, contacts, and other sensitive data outside containers where the information is less secure. [redacted] Consequently, the risky applications we identified may access that information and put ICE data at risk.

- Mobile Device Management: MDM technology can be designed to enforce enterprise security policies on a mobile device. Using MDM, an organization can configure or restrict mobile functionality; security capabilities; and automatically monitor, detect, report, and respond to mobile device policy violations. Even though ICE's MDM provides visibility to all installed applications, ICE did not have a process to periodically review, assess, block, and remove risky applications installed on devices. Additionally [redacted]

- Mobile Threat Defense: Mobile Threat Defense systems are designed to detect the presence of malicious applications, network-based attacks, phishing attacks, improper configurations, and known vulnerabilities in mobile applications or the mobile operating system. Although ICE's Mobile Threat Defense solution can identify and prevent malicious

[12] NIST Special Publication 800-163 Revision 1, *Vetting the Security of Mobile Applications,* April 2019.
[13] DHS Policy Directive 4300A, Attachment CC, *NIST 800-53r5 Control Baselines and ODPs*.

network connections, it is unable to block intrusive functionality from other applications. Additionally, according to ICE's MDM about [redacted] of ICE-managed devices did not have Mobile Threat Defense installed. According to ICE officials, almost all the devices identified without Mobile Threat Defense belong to other DHS agencies and ICE removed the devices from its MDM by the time this alert was issued. The remaining devices, according to ICE officials, did not have Mobile Threat Defense installed due to mission requirements.

Conclusion

ICE CISO staff stated that they have taken actions in response to our recommendations, such as blocking and disabling applications with ties to [redacted], [redacted], and federally prohibited companies; vulnerable messaging applications; and VPN applications. ICE also stated it has taken steps to implement application vetting and is in the process of updating its mobile device use policy. These actions demonstrate progress but do not fully address the risks associated with user-installed applications communicated in this alert. For example, ICE's corrective actions do not fully address removal of risky applications not explicitly identified by DHS OIG or ensure third-party messengers are up to date. ICE and DHS CISO personnel also emphasized that they rely on software security containers and Mobile Threat Defense as mitigating controls. However, our testing of ICE employee devices demonstrated that the devices may store and transmit sensitive device and user data outside the secure containers. In addition, CISA has previously informed Congress that even when implementing technical solutions such as a software container, the downloading of a foreign VPN to Government devices would likely result in data exploitation. Therefore, we are recommending further immediate actions to reduce the risk these user-installed mobile applications pose to ICE's operations, its employees, and the Department.

Recommendations

Recommendation 1: We recommend ICE's Chief Information Officer require the immediate removal of applications that are prohibited by DHS policy, as well as risky and unneeded applications.

Recommendation 2: We recommend ICE's Chief Information Officer immediately assess whether and to what extent risky applications resulted in breaches of sensitive information.

Recommendation 3: We recommend ICE's Chief Information Officer immediately implement a process to assess and reduce risks of user-installed applications on ICE-managed devices.

Recommendation 4: We recommend ICE's Chief Information Officer develop and implement a process to ensure all third-party messenger applications allowed to be used for official duties are up to date with the latest security updates.

Recommendation 5: We recommend ICE's Chief Information Officer update ICE's mobile device use policy to align with current DHS requirements and industry best practices.

Recommendation 6: We recommend the DHS Chief Information Security Officer determine whether similar issues exist for other DHS agencies and take immediate appropriate actions as appropriate.

Management Comments and OIG Analysis

The Director for the DHS Departmental GAO-OIG Liaison Office provided written comments on a draft of this management alert, which are included in their entirety in Appendix B. DHS concurred with our six recommendations. Before we drafted our alert, ICE and DHS provided technical comments. After we issued our draft alert, ICE and DHS provided additional technical comments, including sensitivity concerns. We made revisions and redactions where appropriate. We consider the six recommendations open and resolved.

In its response, DHS disagreed with our conclusion that ICE security controls did not sufficiently reduce the risk to ICE mobile devices and their sensitive information. However, as explained in this management alert, ICE security controls did not prevent employees from downloading onto their mobile devices risky applications designed to share information and sensitive device data with third parties — some of which are adversarial to the U.S. Government. To improve ICE's mitigation controls, we maintain that corrective action is needed, as communicated in the six recommendations.

DHS also expressed accuracy concerns with the percentage of devices we presented that ICE managed without Mobile Threat Defense installed. At the time of our analysis, devices owned by other DHS agencies were managed by ICE's MDM. Accordingly, when we requested data for ICE-managed mobile devices, ICE provided a data set that included devices owned by other DHS agencies. Our analysis and reporting accurately reflects the percentage of devices without Mobile Threat Defense installed for both ICE-owned devices and devices owned by other DHS agencies using the data set as received. After we notified ICE OCIO of our analysis results and before we issued this alert, ICE staff explained they had removed devices owned by other DHS agencies from ICE's MDM. Although these devices are not ICE-owned, they may have risky user-installed applications installed. Therefore, we recommend corrective action to mitigate these risks.

ICE also reported that approximately [redacted] of its devices were exempt from using Mobile Threat Defense. During our ongoing audit, we will request and review documentation supporting this assertion and determine whether ICE had controls in place to review and approve instances in which Mobile Threat Detection was not installed due to mission requirements.

DHS Response to Recommendation 1: Concur. Beginning in July 2023, personnel from ICE OCIO, Office of the Chief Information Security Officer took immediate action to block applications from banned companies, applications developed by known nefarious companies, and VPN applications. Further, ICE OCIO deployed enterprise messaging, directing personnel to uninstall non–mission-related applications from ICE-managed devices; this reduced the number of installations from the users. ICE OCIO is developing an "allowlisting" methodology to block all unapproved applications through automated processes. ICE OCIO is also reviewing risk assessment processes to identify the root cause of how applications were not "blocklisted" on ICE mobile devices from companies on the: (1) *National Defense Authorization Act*, Section 889; (2) the Federal Communications Commission's "List of Equipment and Services Covered By Section 2 of The Secure Networks Act;" (3) *Secure and Trusted Communications Networks Act of 2019*; or (4) CISA Binding Operational Directives. Finally, ICE OCIO is developing a Cybersecurity Supply Chain Risk Management (C-SCRM) capability to assess supply chain threats and vulnerabilities. Estimated Completion Date: March 29, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which we consider open and resolved. This recommendation will remain open and resolved until we receive evidence of application removal, ICE's "allowlisting" methodology and implementation, and the results and course of action from the risk assessment process review.

DHS Response to Recommendation 2: Concur. Through ICE's robust, multi-tiered defense and in-depth strategy, the device and applications are continuously monitored for abnormal behavior or changes to configurations. For example, the ICE Mobile Threat Detection solution is intended to detect unexpected interactions with applications or malicious network connections. Beginning in August 2023, ICE proactively conducted forensics on several devices containing banned applications and applications from known nefarious sources, including reviews of logs, and no evidence of nefarious activity was discovered. ICE will continue to report through normal incident response channels if data breach incidents are identified, and ICE will provide the OIG with documentation of these efforts, as appropriate. Estimated Completion Date: November 30, 2023.

OIG Analysis: ICE's actions are responsive to this recommendation, which we consider open and resolved. This recommendation will remain open and resolved until we receive evidence of and assess the extent of ICE's forensic analysis and related efforts.

DHS Response to Recommendation 3: Concur. Beginning in July 2023, ICE OCIO initiated efforts to assess and reduce the risks of user-installed applications on ICE-managed devices. As part of this effort, ICE is using NIST SP 800-124, Revision 2, as guidance to further enhance the ICE mobile security program. ICE will further invest in a mobile application vetting (MAV) solution. Specifically, in February 2023, ICE OCIO received access to the CISA MAV tool for vetting of ICE internally-developed mobile applications. Going forward, ICE OCIO will develop a process to use this capability to review third-party applications. In addition, ICE met with DHS OCIO to learn about DHS OCIO's mobile device management "allowlisting" program and reviewed the DHS mobile application risk assessment process. With this knowledge and keeping with the current Corporate-Owned Personally Enabled model, ICE will research and determine if a "blocklisting" or "allowlisting" approach will meet operational needs. Finally, ICE will develop a C-SCRM capability that will assess supply chain threats and vulnerabilities. Estimated Completion Date: March 29, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which we consider open and resolved. This recommendation will remain open and resolved until we receive evidence of ICE's implementation of proposed actions, including results and a plan of action from ICE OCIO's review of "current capabilities allowed for ICE mission data inside and outside the containers" as stated in the introductory paragraphs of DHS' management response.

DHS Response to Recommendation 4: Concur. ICE OCIO will investigate and implement an automated solution to force device configurations to automatically update third-party applications, through the native application store. The agency currently manages agency-owned application "versioning" through ICE's MDM solution. Estimated Completion Date: March 29, 2024.

OIG Analysis: ICE's proposed actions are responsive to this recommendation, which we consider open and resolved. This recommendation will remain open and resolved until we receive evidence that ICE has implemented the solution.

DHS Response to Recommendation 5: Concur. ICE drafted an updated agency mobile use policy, which is currently in the peer review process. Once the review process is completed, the policy will be routed for OCIO and ICE Policy approval. Estimated Completion Date: February 29, 2024.

OIG Analysis: ICE's proposed actions are responsive to this recommendation, which we consider open and resolved. This recommendation will remain open and resolved until we receive and review the updated mobile use policy.

DHS Response to Recommendation 6: Concur. DHS OCIO will implement the following steps to address this recommendation: 1) ensure coverage of all DHS mobile devices through an authorized DHS MDM system; 2) evaluate and consider additional technical controls, such as an enterprise “allowlist” policy; and 3) review the existing DHS mobile device policy, DHS Policy Directive 4300A, *DHS Sensitive Systems*, Version 13.1, dated July 27, 2017, and associated attachments, and update each as appropriate. Estimated Completion Date: March 29, 2024.

OIG Analysis: DHS’ proposed actions are responsive to this recommendation, which we consider open and resolved. This recommendation will remain open and resolved until we receive evidence of DHS’ evaluation of other DHS agencies’ user-installed application risks and implementation of appropriate actions.

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), which amended the *Inspector General Act of 1978*.

We issued this management alert as part of an ongoing audit of ICE's mobile device management and security. The objective of our ongoing audit is to determine the extent to which ICE manages and secures its mobile devices. As part of our audit, from April 27 to August 17, 2023, we met with ICE OCIO officials and staff within the Information Assurance Division, Systems Engineering Division, Security Assurance Branch, Enterprise Services Branch, ICE SOC, ICE Homeland Security Investigations, and the DHS Chief Information Security Officer. We conducted limited physical testing of ICE devices with ICE supervision, reviewed system settings, used mobile applications, and took screenshots of results.

We requested a listing of all personal applications installed on mobile devices identified by the ICE MDM system. ICE officials explained they could provide a report of all the mobile applications but could not provide a report identifying which devices had specific applications installed. The report identified the application name, package ID, installed version, source name, and number of installs of each application. Therefore, although unable to tie applications to specific devices, we were able to review the total number of applications installed across the entire population of devices managed by the ICE MDM. The data allowed us to quantify the number of devices with a specific application installed by equating one install to one device. However, when reporting on applications grouped by category, such as the number of devices with a file sharing application, we did not equate application installs to a device. We did this because each device could have multiple applications from a grouped category. We performed a limited data reliability assessment by comparing MDM report figures to observations we made during a presentation of the ICE MDM. We considered the information in the report to be sufficiently reliable for purposes of our limited test. The report is a snapshot in time as of April 27, 2023.

We reviewed the various types of applications by their application names and package ID and conducted open-source research available through application stores, commercial websites, and application developer guide documents. We also reviewed NIST's known vulnerability database, CISA directives, public laws, and DHS and ICE mobile device policies. After completing our analysis, we confirmed our findings with ICE OCIO officials, discussed their planned corrective actions, and decided to issue this alert due to the potential immediate impacts on ICE mobile device security.

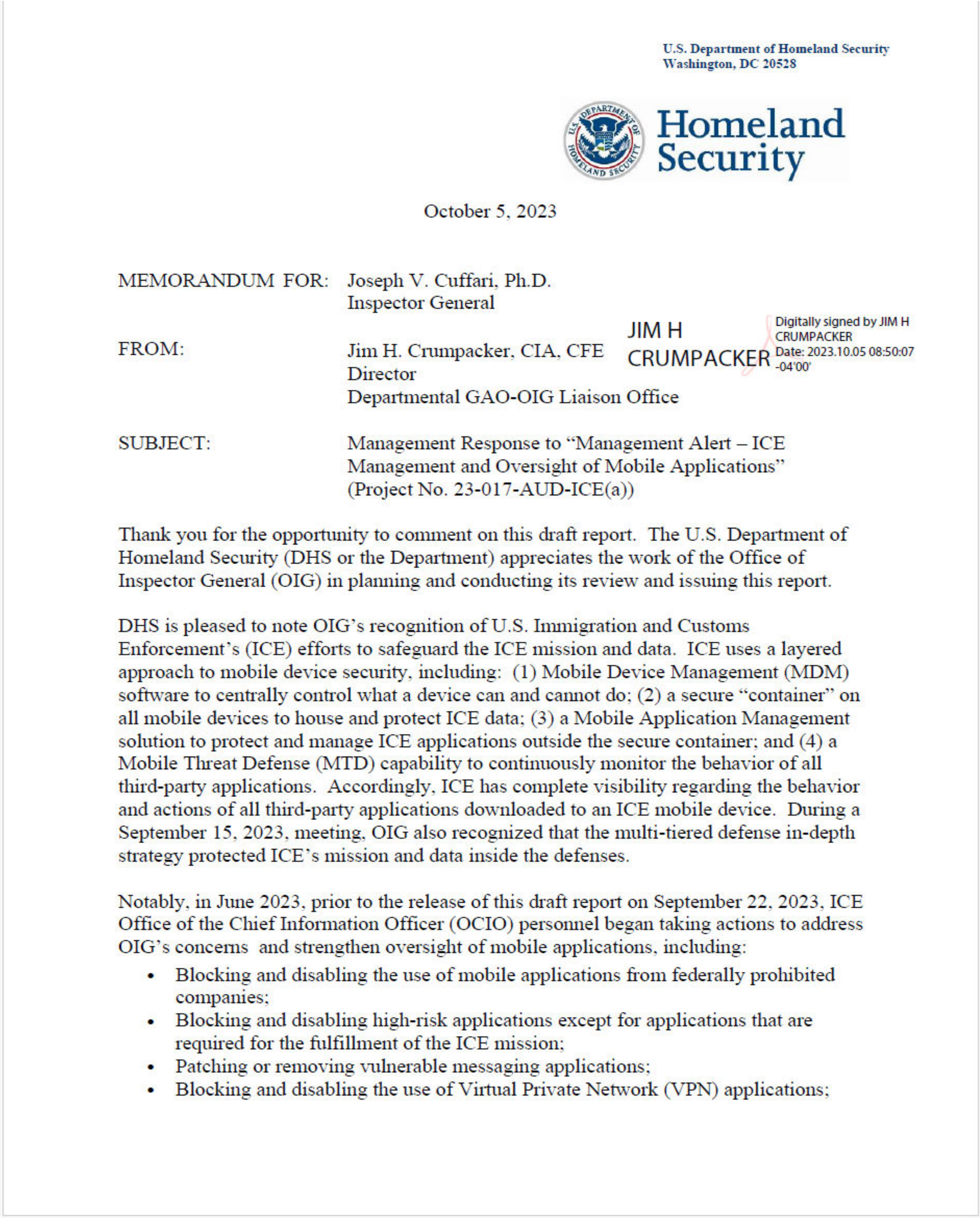
We conducted this work pursuant to the *Inspector General Act of 1978,* 5 U.S.C. §§ 401–424, and in connection with an ongoing audit being performed according to generally accepted government auditing standards. Those standards require we plan and perform our audit work to obtain sufficient, appropriate 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 Access to DHS Information

During this review, DHS provided timely responses to our requests for information from the mobile device management system. However, we experienced delays and denials not associated with this management alert, which we will describe in the final report.

Appendix B:
DHS Comments on the Draft Report



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

Homeland Security

October 5, 2023

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: 2023.10.05 08:50:07 -04'00'

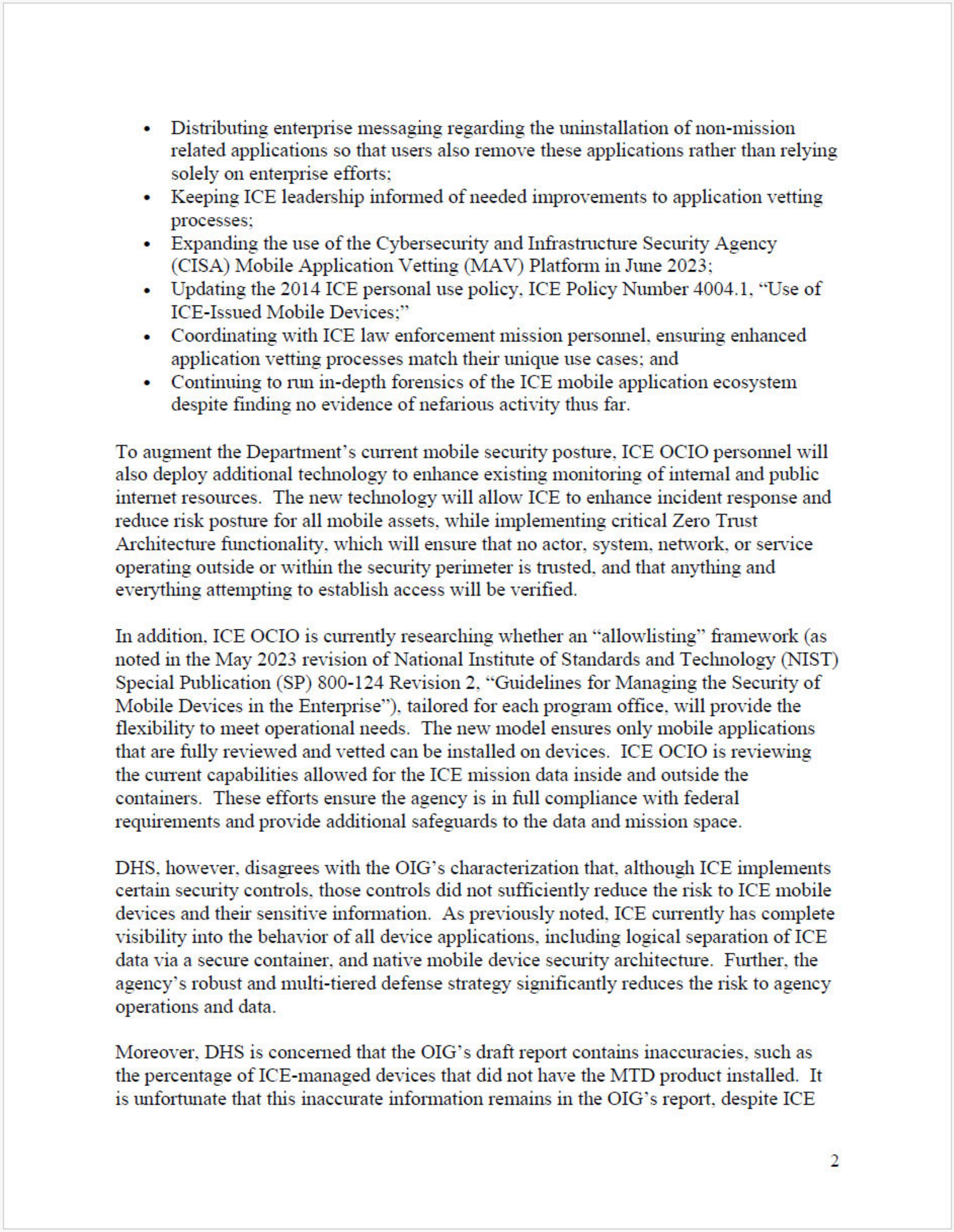
SUBJECT: Management Response to "Management Alert – ICE Management and Oversight of Mobile Applications" (Project No. 23-017-AUD-ICE(a))

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.

DHS is pleased to note OIG's recognition of U.S. Immigration and Customs Enforcement's (ICE) efforts to safeguard the ICE mission and data. ICE uses a layered approach to mobile device security, including: (1) Mobile Device Management (MDM) software to centrally control what a device can and cannot do; (2) a secure "container" on all mobile devices to house and protect ICE data; (3) a Mobile Application Management solution to protect and manage ICE applications outside the secure container; and (4) a Mobile Threat Defense (MTD) capability to continuously monitor the behavior of all third-party applications. Accordingly, ICE has complete visibility regarding the behavior and actions of all third-party applications downloaded to an ICE mobile device. During a September 15, 2023, meeting, OIG also recognized that the multi-tiered defense in-depth strategy protected ICE's mission and data inside the defenses.

Notably, in June 2023, prior to the release of this draft report on September 22, 2023, ICE Office of the Chief Information Officer (OCIO) personnel began taking actions to address OIG's concerns and strengthen oversight of mobile applications, including:

- Blocking and disabling the use of mobile applications from federally prohibited companies;
- Blocking and disabling high-risk applications except for applications that are required for the fulfillment of the ICE mission;
- Patching or removing vulnerable messaging applications;
- Blocking and disabling the use of Virtual Private Network (VPN) applications;



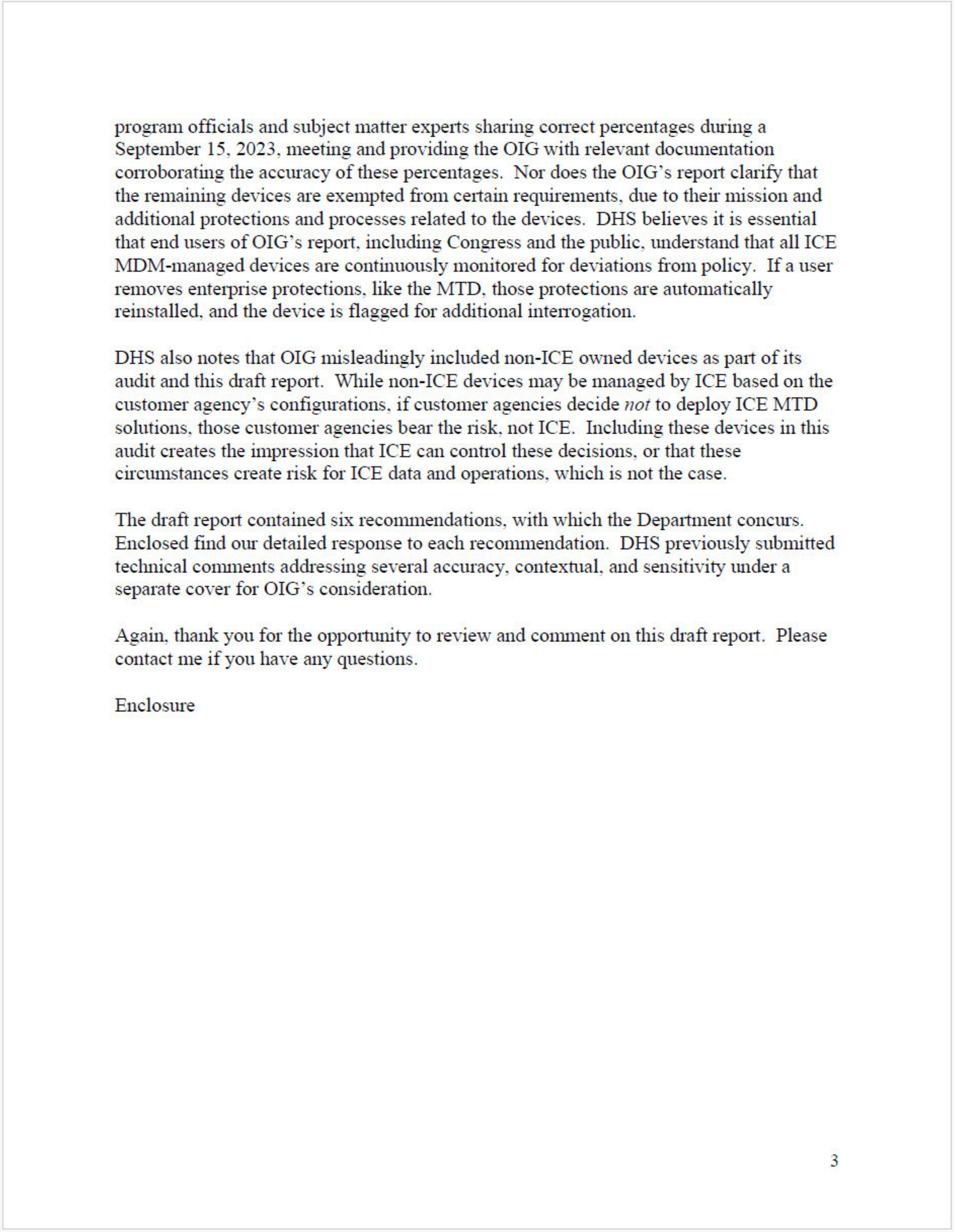
- Distributing enterprise messaging regarding the uninstallation of non-mission related applications so that users also remove these applications rather than relying solely on enterprise efforts;
- Keeping ICE leadership informed of needed improvements to application vetting processes;
- Expanding the use of the Cybersecurity and Infrastructure Security Agency (CISA) Mobile Application Vetting (MAV) Platform in June 2023;
- Updating the 2014 ICE personal use policy, ICE Policy Number 4004.1, "Use of ICE-Issued Mobile Devices;"
- Coordinating with ICE law enforcement mission personnel, ensuring enhanced application vetting processes match their unique use cases; and
- Continuing to run in-depth forensics of the ICE mobile application ecosystem despite finding no evidence of nefarious activity thus far.

To augment the Department's current mobile security posture, ICE OCIO personnel will also deploy additional technology to enhance existing monitoring of internal and public internet resources. The new technology will allow ICE to enhance incident response and reduce risk posture for all mobile assets, while implementing critical Zero Trust Architecture functionality, which will ensure that no actor, system, network, or service operating outside or within the security perimeter is trusted, and that anything and everything attempting to establish access will be verified.

In addition, ICE OCIO is currently researching whether an "allowlisting" framework (as noted in the May 2023 revision of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-124 Revision 2, "Guidelines for Managing the Security of Mobile Devices in the Enterprise"), tailored for each program office, will provide the flexibility to meet operational needs. The new model ensures only mobile applications that are fully reviewed and vetted can be installed on devices. ICE OCIO is reviewing the current capabilities allowed for the ICE mission data inside and outside the containers. These efforts ensure the agency is in full compliance with federal requirements and provide additional safeguards to the data and mission space.

DHS, however, disagrees with the OIG's characterization that, although ICE implements certain security controls, those controls did not sufficiently reduce the risk to ICE mobile devices and their sensitive information. As previously noted, ICE currently has complete visibility into the behavior of all device applications, including logical separation of ICE data via a secure container, and native mobile device security architecture. Further, the agency's robust and multi-tiered defense strategy significantly reduces the risk to agency operations and data.

Moreover, DHS is concerned that the OIG's draft report contains inaccuracies, such as the percentage of ICE-managed devices that did not have the MTD product installed. It is unfortunate that this inaccurate information remains in the OIG's report, despite ICE



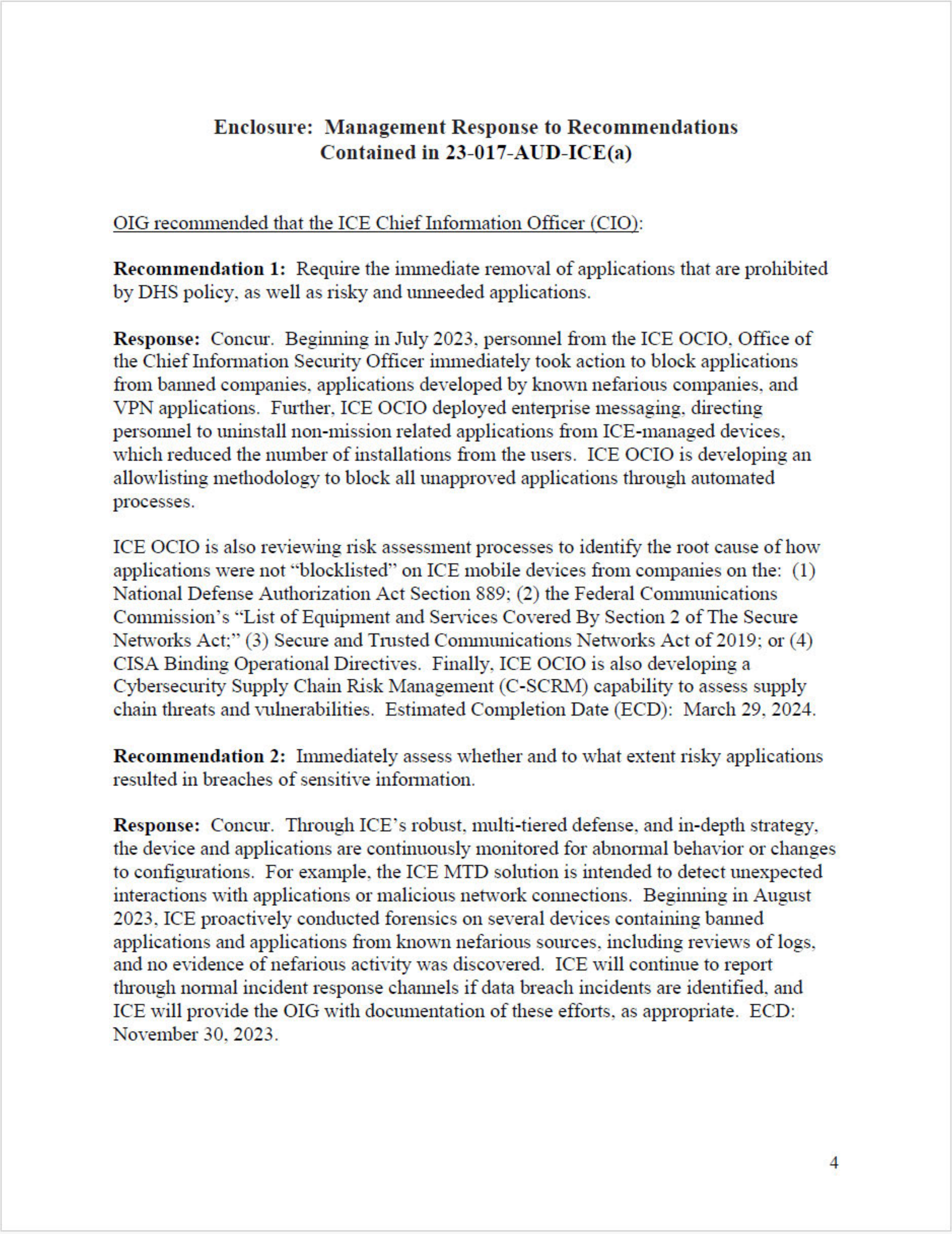
program officials and subject matter experts sharing correct percentages during a September 15, 2023, meeting and providing the OIG with relevant documentation corroborating the accuracy of these percentages. Nor does the OIG's report clarify that the remaining devices are exempted from certain requirements, due to their mission and additional protections and processes related to the devices. DHS believes it is essential that end users of OIG's report, including Congress and the public, understand that all ICE MDM-managed devices are continuously monitored for deviations from policy. If a user removes enterprise protections, like the MTD, those protections are automatically reinstalled, and the device is flagged for additional interrogation.

DHS also notes that OIG misleadingly included non-ICE owned devices as part of its audit and this draft report. While non-ICE devices may be managed by ICE based on the customer agency's configurations, if customer agencies decide *not* to deploy ICE MTD solutions, those customer agencies bear the risk, not ICE. Including these devices in this audit creates the impression that ICE can control these decisions, or that these circumstances create risk for ICE data and operations, which is not the case.

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

Again, thank you for the opportunity to review and comment on this draft report. Please contact me if you have any questions.

Enclosure



Enclosure: Management Response to Recommendations Contained in 23-017-AUD-ICE(a)

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

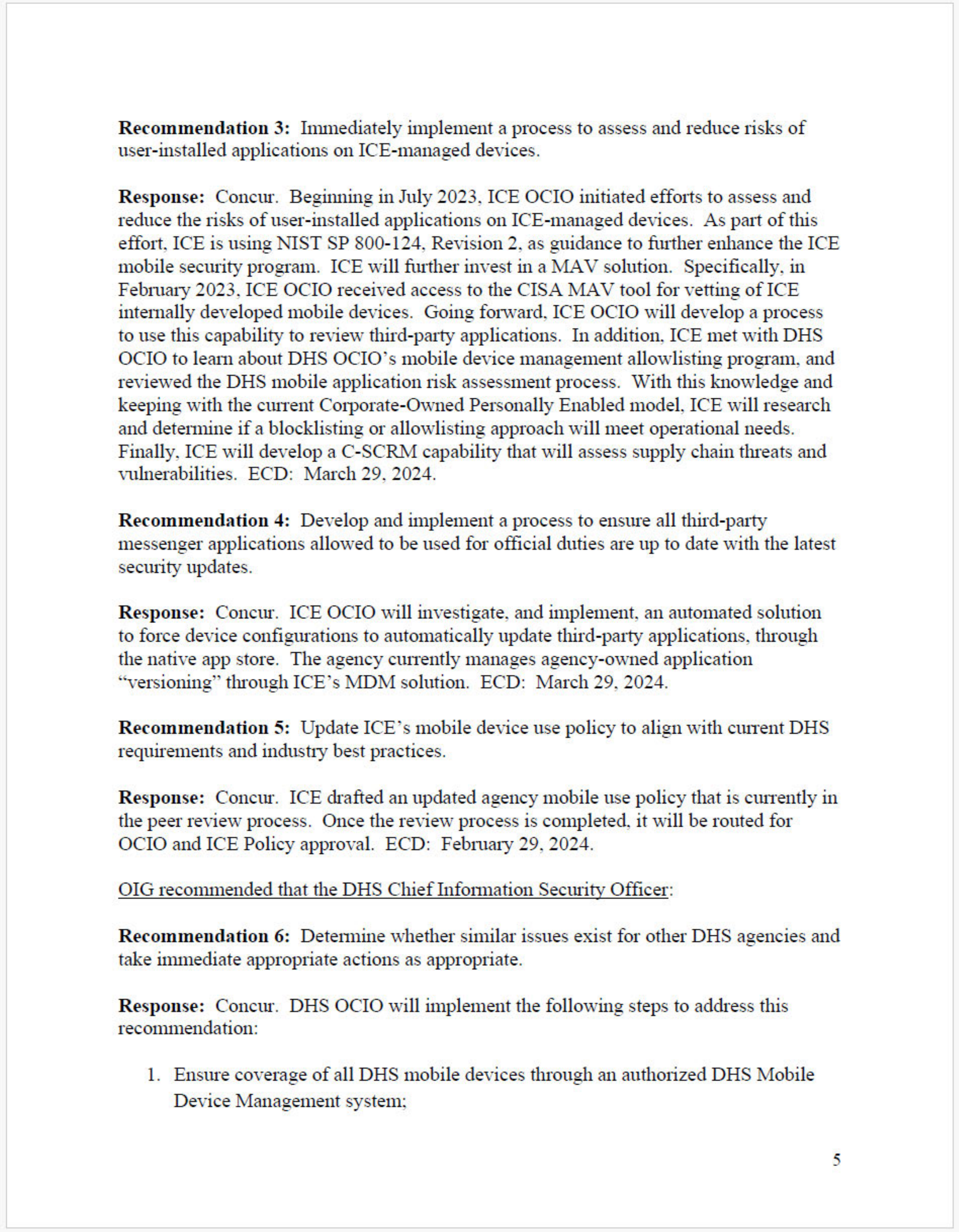
Recommendation 1: Require the immediate removal of applications that are prohibited by DHS policy, as well as risky and unneeded applications.

Response: Concur. Beginning in July 2023, personnel from the ICE OCIO, Office of the Chief Information Security Officer immediately took action to block applications from banned companies, applications developed by known nefarious companies, and VPN applications. Further, ICE OCIO deployed enterprise messaging, directing personnel to uninstall non-mission related applications from ICE-managed devices, which reduced the number of installations from the users. ICE OCIO is developing an allowlisting methodology to block all unapproved applications through automated processes.

ICE OCIO is also reviewing risk assessment processes to identify the root cause of how applications were not "blocklisted" on ICE mobile devices from companies on the: (1) National Defense Authorization Act Section 889; (2) the Federal Communications Commission's "List of Equipment and Services Covered By Section 2 of The Secure Networks Act;" (3) Secure and Trusted Communications Networks Act of 2019; or (4) CISA Binding Operational Directives. Finally, ICE OCIO is also developing a Cybersecurity Supply Chain Risk Management (C-SCRM) capability to assess supply chain threats and vulnerabilities. Estimated Completion Date (ECD): March 29, 2024.

Recommendation 2: Immediately assess whether and to what extent risky applications resulted in breaches of sensitive information.

Response: Concur. Through ICE's robust, multi-tiered defense, and in-depth strategy, the device and applications are continuously monitored for abnormal behavior or changes to configurations. For example, the ICE MTD solution is intended to detect unexpected interactions with applications or malicious network connections. Beginning in August 2023, ICE proactively conducted forensics on several devices containing banned applications and applications from known nefarious sources, including reviews of logs, and no evidence of nefarious activity was discovered. ICE will continue to report through normal incident response channels if data breach incidents are identified, and ICE will provide the OIG with documentation of these efforts, as appropriate. ECD: November 30, 2023.



Recommendation 3: Immediately implement a process to assess and reduce risks of user-installed applications on ICE-managed devices.

Response: Concur. Beginning in July 2023, ICE OCIO initiated efforts to assess and reduce the risks of user-installed applications on ICE-managed devices. As part of this effort, ICE is using NIST SP 800-124, Revision 2, as guidance to further enhance the ICE mobile security program. ICE will further invest in a MAV solution. Specifically, in February 2023, ICE OCIO received access to the CISA MAV tool for vetting of ICE internally developed mobile devices. Going forward, ICE OCIO will develop a process to use this capability to review third-party applications. In addition, ICE met with DHS OCIO to learn about DHS OCIO's mobile device management allowlisting program, and reviewed the DHS mobile application risk assessment process. With this knowledge and keeping with the current Corporate-Owned Personally Enabled model, ICE will research and determine if a blocklisting or allowlisting approach will meet operational needs. Finally, ICE will develop a C-SCRM capability that will assess supply chain threats and vulnerabilities. ECD: March 29, 2024.

Recommendation 4: Develop and implement a process to ensure all third-party messenger applications allowed to be used for official duties are up to date with the latest security updates.

Response: Concur. ICE OCIO will investigate, and implement, an automated solution to force device configurations to automatically update third-party applications, through the native app store. The agency currently manages agency-owned application "versioning" through ICE's MDM solution. ECD: March 29, 2024.

Recommendation 5: Update ICE's mobile device use policy to align with current DHS requirements and industry best practices.

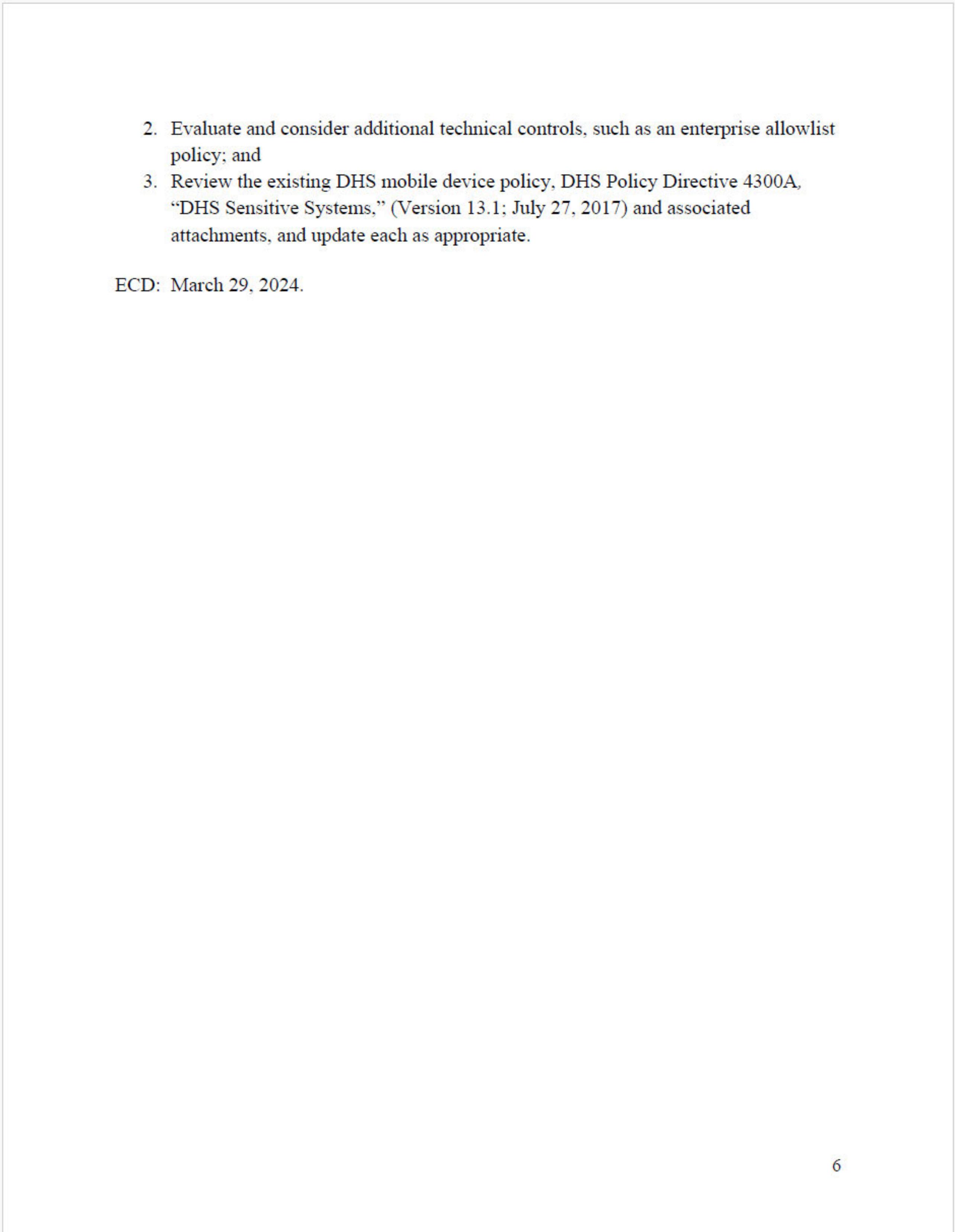
Response: Concur. ICE drafted an updated agency mobile use policy that is currently in the peer review process. Once the review process is completed, it will be routed for OCIO and ICE Policy approval. ECD: February 29, 2024.

<u>OIG recommended that the DHS Chief Information Security Officer</u>:

Recommendation 6: Determine whether similar issues exist for other DHS agencies and take immediate appropriate actions as appropriate.

Response: Concur. DHS OCIO will implement the following steps to address this recommendation:

1. Ensure coverage of all DHS mobile devices through an authorized DHS Mobile Device Management system;



2. Evaluate and consider additional technical controls, such as an enterprise allowlist policy; and
3. Review the existing DHS mobile device policy, DHS Policy Directive 4300A, "DHS Sensitive Systems," (Version 13.1; July 27, 2017) and associated attachments, and update each as appropriate.

ECD: March 29, 2024.

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
ICE Office of Chief Information Officer
ICE Component Liaison

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