Report No. DODIG-2023-041

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

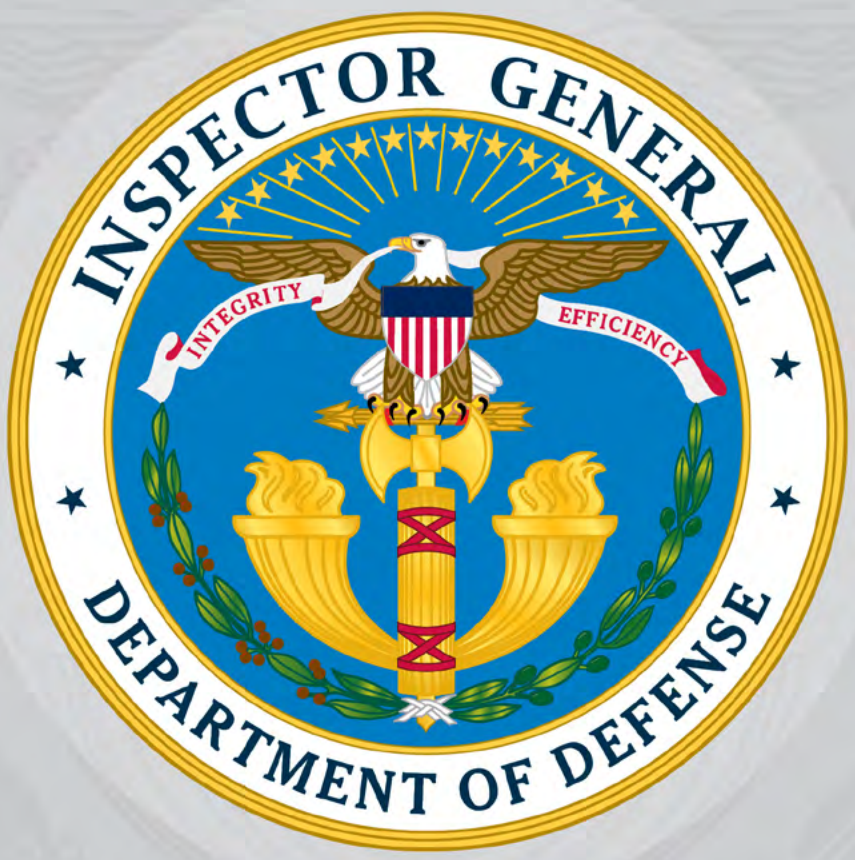
FEBRUARY 9, 2023

(U) Management Advisory: The DoD's Use of Mobile Applications

~~Controlled by: Audit/Cyberspace Operations~~
~~CUI Category: OPSEC, ISVI~~
~~Distribution/Dissemination Control: FEDCON~~
~~POC: Assistant Inspector General for Audit, Cyberspace Operations & Acquisition, Contracting, and Sustainment,~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

February 9, 2023

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY
CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, CHIEF DIGITAL AND ARTIFICIAL INTELLIGENCE OFFICE DIRECTORATE FOR DIGITAL SERVICES

(U) SUBJECT: Management Advisory: The DoD's Use of Mobile Applications (Report No. DODIG-2023-041)

(U) The purpose of this management advisory is to provide DoD officials responsible for approving and managing the use of mobile applications with concerns identified during the Audit of the Defense Digital Service Support of DoD Programs and Operations (Project No. D2021-D000CU-0143.000). Specifically, we determined that DoD personnel are conducting official business on their DoD mobile devices using mobile applications in violation of Federal and DoD electronic messaging and records retention policies. In addition, DoD personnel are downloading mobile applications to their DoD mobile devices that could pose operational and cybersecurity risks to DoD information and information systems. We prepared this management advisory with integrity, objectivity, and independence, as required by the Council of the Inspectors General on Integrity and Efficiency's Quality Standards for Federal Offices of Inspector General.

(U) We provided a draft copy of this management advisory to DoD management and requested written comments on the findings and recommendations. We considered management's comments on the draft when preparing the final management advisory. Those comments are included in the management advisory. The draft copy of the management advisory included three appendixes containing listings of the mobile applications offered to or installed by DoD Components; therefore, the management comments include references to Appendixes A, B, and C. However, based on operational security concerns identified by DoD Components during their security reviews, we made the decision to remove the Appendixes from the final management advisory.

(U) This management advisory contains 14 recommendations that we consider unresolved because management officials did not fully address or did not respond to the recommendations. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this advisory, the recommendations will remain unresolved until an agreement is reached on the actions to be taken to address the recommendations. Once an agreement is reached, the recommendations will be considered resolved but open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) This management advisory contains two recommendations that we consider resolved. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this advisory, the recommendations will remain open until documentation is submitted showing that the agreed-upon actions are complete. Once we verify that the actions are complete, the recommendations will be closed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, within 30 days please provide us your comments concerning specific actions in process or alternative corrective actions proposed on the recommendations. For the resolved recommendations, within 90 days please provide us documentation showing that the agreed-upon action has been completed. Your response should be sent as a PDF file to followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

(U) We appreciate the cooperation and assistance received during the review. If you have any questions, please contact me at [redacted].

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations & Acquisition,
Contracting, and Sustainment

(U) Background

(U) On August 2, 2021, we announced the "Audit of the Defense Digital Service Support of DoD Programs and Operations," (Project No. D2021-D000CU-0143.000). The objective of the audit is to determine whether Defense Digital Service (DDS) engagements have achieved their intended purpose and were executed in accordance with DoD and Federal policies. During the audit, we determined that the former DDS Director authorized the use of an unmanaged mobile application for official DoD business, in violation of DoD electronic messaging and records retention policies.[1] The use of unmanaged applications to conduct official business poses operational and cybersecurity risks and could result in users inadvertently revealing sensitive DoD information or introducing malware to DoD information systems. Therefore, we expanded our review beyond the DDS to determine whether the misuse of unmanaged applications for official business on DoD mobile devices is a DoD enterprise-wide concern.[2] This management advisory details the results of that expanded review and provides recommendations for corrective action, that when complete, should limit the unjustified use of unmanaged applications on DoD mobile devices and reduce the associated risks.

(U) DoD Mobile Device and Application Management

(U) DoD Components procure commercial off-the-shelf mobile devices and cellular service and provide the mobile devices to select personnel to conduct official DoD business. DoD Components can manage, configure, and secure the mobile devices internally with DoD-approved mobile device management software or subscribe to the DoD Mobility Unclassified Capability (DMUC) service, which is operated by the Defense Information Systems Agency (DISA).

~~(CUI)~~ DoD Components that manage their mobile devices internally can allow or restrict user access to public application stores. The Components can also create and control [redacted] and centralized repositories, or stores, of selected applications that Component personnel can access.[3] DoD Component officials can also remotely remove or hide applications from users' devices if the Component determines that the application poses an operational or cybersecurity risk.[4]

[1] (U) A mobile application is a software program installed on a device with a mobile operating system, such as Apple iOS and Android. For the purposes of this advisory, the term "managed" refers to mobile applications approved by DoD Components for official DoD business; "authorized unmanaged" refers to mobile applications authorized by DoD Components for personal use on DoD devices; and "unauthorized unmanaged" refers to mobile applications that are downloaded from public application stores and cannot be used to conduct official DoD business or for personal use on DoD mobile devices because they have not been assessed by the DoD. For the purposes of this advisory, official DoD business includes unclassified and controlled unclassified information.

[2] (U) A mobile device is a portable computing device with communication capabilities, such as a smart phone or tablet.

[3] ~~(CUI)~~ [redacted]

[4] (U) Hiding means removing the application's icon from the device's display.

(U) DoD Components that subscribe to the DMUC do not have direct control over their users' access to mobile applications. DISA operates the DMUC service and provides DMUC users with unrestricted access to public application stores, as well as access to the DMUC application stores, such as the DoD Mobile Application Store and Personal Use Mobile Application (PUMA) store. DISA includes applications in the DMUC application stores after receiving a request for the application from a DoD Component and assessing the application for security risks. According to DISA's Enterprise Integration and Innovation Center Director/Chief Information Officer (CIO), DISA can remotely remove managed mobile applications from users' devices and hide unmanaged applications from users through the DMUC. The DISA CIO also stated that for unmanaged applications, DoD Components can only request that users remove the applications from their devices. However, the DISA CIO stated that DoD Components can indirectly control users' access to mobile applications through Component-level mobile application policy, user training, and reports of users' downloaded mobile applications.

(U) DoD Mobile Applications

(U) The DoD separates mobile device applications into two primary categories, managed and unmanaged.[5] Unmanaged mobile device applications are further separated into two subcategories, authorized and unauthorized. Managed applications can be used to conduct official DoD business. The DoD Components must conduct a cybersecurity assessment or use existing assessment results before approving managed applications. The managed applications allow mobile device users to access controlled unclassified information (CUI) on the mobile device or connect to DoD networks that contain CUI.[6] The DoD Components control managed applications through their own mobile application management systems unless they use the DMUC. DISA controls the managed applications for the DoD Components that use the DMUC. Users download the managed applications from a managed application store maintained by their Component or DISA.

(U) Authorized unmanaged applications cannot be used for official DoD business but are allowed to be used for personal use on DoD mobile devices. Users typically download unmanaged applications from public application stores, including through DISA's PUMA store that consists of links to the applications in the public application stores. The DoD Components must configure their mobile devices to segregate unmanaged applications to prevent them from accessing CUI data on the device or connecting to DoD systems that contain CUI. Although the DoD Components, including DISA, are not required to conduct a cybersecurity assessment or review existing assessments of unmanaged applications, the authorizing official must assume the cybersecurity risks of allowing unmanaged applications to be installed

[5] (U) The categories describe the different groups of mobile applications based on our audit analysis.

[6] (U) CUI is information the U.S. Government creates or possesses, or that an entity creates or possesses for or on behalf of the U.S. Government, that a law, regulation, or U.S. Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

(U) on DoD mobile devices. In addition, the users must sign a user agreement acknowledging that they received training on the operational security risks introduced by unmanaged applications, including applications that use the global positioning system (GPS).

(U) Unauthorized unmanaged applications cannot be used to conduct official DoD business or for personal use on DoD mobile devices. Examples of unauthorized unmanaged applications include games, shopping, and other entertainment applications. Users typically download unauthorized unmanaged applications from public application stores to their DoD mobile devices.

(U) DoD Guidance on the Use of Mobile Devices and Applications

(U) DoD guidance on the use of mobile devices and applications is contained in DoD Regulations, Instructions, and memorandums. The DoD CIO memorandum, "Mobile Application Security Requirements," (DoD CIO memorandum) requires DoD Components, including DISA, to follow the evaluation, security, and training requirements for the use of mobile devices and applications in the DoD.[7] The memorandum states that personal use of mobile applications must comply with DoD Regulation 5500.07-R, "Joint Ethics Regulation."[8]

(U) DoD Regulation 5500.07-R states that government-owned communication systems and equipment (including mobile devices) should be for official use and authorized purposes only.[9] The Regulation states that official use includes emergency communications and communications that the DoD Component determines are necessary in the interest of the U.S. Government. The Regulation further states that official use may include communications by deployed military and DoD personnel, in the interest of morale and welfare, when approved by the theater commanders. Authorized purposes are defined as brief communications made by DoD personnel while they are traveling on government business and personal communications made while at the work place.[10]

(U) DoD Instruction (DoDI) 8170.01, "Online Information Management and Electronic Messaging," is specific to the use of electronic messaging services, such as electronic mail, texting, and chat communications.[11] DoDI 8170.01 assigns responsibility for establishing guidance for protecting CUI to the Under Secretary of Defense for Intelligence and Security. DoDI 8170.01 prohibits the use of non–DoD-controlled electronic messaging services to process non-public DoD information and the use of personal, non-official electronic messaging

[7] (U) DoD Chief Information Officer memorandum, "Mobile Application Security Requirements," October 6, 2017.

[8] (U) DoD Regulation 5500.07-R, "Joint Ethics Regulation," August 30, 1993 (Incorporating Change 7, November 17, 2011).

[9] (U) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, (Incorporating Change 1, August 24, 2021) defines official use as authorized communications or activities conducted as an assigned DoD personnel function.

[10] (U) According to DoD Regulation 5500.07-R, examples of personal communications include checking in with spouse or minor children, scheduling doctor and auto or home repair appointments, brief Internet searches, and e-mailing directions to visiting relatives.

[11] (U) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, (Incorporating Change 1, August 24, 2021).

(U) accounts to conduct official DoD business.[12] DoDI 8170.01 also requires all records, whether online or created and sent using official or personal electronic messaging services, to comply with DoDI 5015.02, "DoD Records Management Program," implementing Public Law 113-187.[13] DoDI 5015.02 states that records created using any electronic applications or electronic messaging accounts must be managed and maintained in accordance with National Archives and Records Administration guidance.[14] The National Archives and Records Administration guidance requires that Components retain electronic messaging records for a minimum of 7 years.

(U) Records are evidence of DoD Component organization, functions, policies, procedures, decisions, and activities. DoDI 5015.02 states that effective and efficient management of records provides the information for decision-making at all levels, mission planning and operations, business continuity, and preservation of U.S. history. According to the Office of Management and Budget and the National Archives and Records Administration, well-managed records can be used to assess the impact of a program, improve business processes, protect the rights and interest of people, and hold DoD officials accountable for their actions.[15] The retention of electronic messaging records facilitates compliance with Section 552, title 5, United States Code, 2020, commonly known as the Freedom of Information Act (FOIA), which states that each Federal agency must make records promptly available to any person upon request with limited exceptions.

(U) In 2016 and 2018, after DoD and U.S. Government officials, including the Secretary of Defense, were found to have used their personal e-mail accounts to conduct official business, the Deputy Secretary of Defense and the DoD CIO issued memorandums reminding DoD employees that the use of non-official (non–DoD-controlled) electronic messaging accounts to conduct official DoD business is prohibited. The DoD also issued a memorandum concerning the use of mobile devices and applications, in response to operational concerns. In 2018, the Deputy Secretary of Defense issued a memorandum on the "Use of Geolocation-Capable Devices, Applications, and Services" that prohibits the use of geolocation features and functionality on government-issued and personal devices and applications in operational areas.[16] The memorandum states that geolocation features and functionality can expose personal information, locations, routines, and numbers of DoD personal and potentially create unintended security consequences and increased risk to the mission.

---

[12] (U) DoDI 8170.01 uses the term "non-DoD-controlled" and "non-official" for authorized and unauthorized unmanaged applications. Non-public information is defined as information generally not available to the public, obtained in the course of one's official DoD duties or position, which would normally not be releasable under the Freedom of Information Act, section 552, title 5, United States Code (2020).

[13] (U) DoDI 5015.02, "DoD Records Management Program," February 24, 2015, (Incorporating Change 1, August 17, 2017). Public Law 113-187, "Presidential and Federal Records Act Amendments of 2014," November 26, 2014.

[14] (U) National Archives and Records Administration, "General Records Schedule 6.1," as of April 2020.

[15] (U) Office of Management and Budget M-12-18, "Managing Government Records Directive," August 24, 2012.

[16] (U) Deputy Secretary of Defense memorandum, "Use of Geolocation-Capable Devices, Applications, and Services," August 3, 2018. "Operational area" is defined as a geographic area in which military operations are conducted.

(U) Mobile Application Review Methodology

(U) To determine whether the misuse of unmanaged applications on DoD mobile devices was a DoD enterprise-wide concern, we interviewed officials from the Office of the DoD CIO, the National Security Agency, DISA, and the DDS to understand the processes and procedures related to the use of mobile applications across the DoD. We also obtained mobile application request data, mobile application data, and user download data from DISA to identify the applications intended to be used for official DoD business.

(U) The DoD Does Not Have Adequate Controls over the Use of Mobile Applications

(U) DoD Component personnel used unmanaged electronic messaging applications in violation of Federal and DoD electronic messaging and records retention policies. In addition, DoD Components:

- (U) allowed personnel to have unrestricted access to unauthorized unmanaged applications through public application stores that could pose operational and cybersecurity risks;
- (U) offered authorized unmanaged mobile applications through application stores that pose known operational and cybersecurity risks to DoD information and systems; and
- (U) lacked controls to ensure personal use of DoD devices was limited and did not pose operational and cybersecurity risks to the DoD.

(U) DoD personnel violated policy and misused mobile applications because the DoD does not have a comprehensive mobile device and application policy that addresses the operational and cybersecurity risks associated with the use of mobile devices and applications. In addition, DISA and other DoD Components do not provide adequate training on the acceptable use of DoD mobile devices or applications. Contributing to the issue, DoD mobile device users cannot easily identify which of the mobile applications on their DoD mobile devices have been approved for official DoD business.

(U) As a result, the DoD Components' mobile device programs vary widely in the features and applications that users are permitted to access and use. DoD officials may not be aware of the operational and cybersecurity risks that unmanaged applications pose to the DoD. DoD personnel may inadvertently lose or intentionally delete important DoD communications on unmanaged messaging applications. Additionally, mobile applications that are misused by DoD personnel or are compromised by malicious actors can expose DoD information or introduce malware to DoD systems.

(U) Unmanaged Electronic Messaging Applications Used in Violation of Policy

(U) DoD Component personnel used unmanaged electronic messaging applications to conduct official DoD business in violation of Federal and DoD electronic messaging and records retention policies. DoDI 8170.01, "Online Information Management and Electronic Messaging," states that non–DoD-controlled electronic messaging services, regardless of the perceived

(U) security of the service, cannot be used to communicate non-public DoD information.[17] The Instruction also prohibits the use of personal, non-official electronic messaging accounts to conduct official DoD business for personal convenience or preference. DoDI 8170.01 states that if non–DoD-controlled electronic messaging services are used to conduct official business, the user must comply with Federal and DoD records retention policies, such as DoDI 5015.02. DoDI 5015.02 also prohibits the use of non-official electronic messaging accounts to conduct official DoD business, with limited exceptions.[18] However, if DoD personnel use a non-official account, DoDI 5015.02 requires that they forward the message to an official electronic messaging account within 20 days of the original record's creation. DoDI 5015.02 also requires that records created using any electronic applications or electronic messaging accounts must be managed and retained for a minimum of 7 years according to National Archives and Records Administration guidance. However, the DoD has no assurance that DoD personnel are forwarding DoD information created or sent on unmanaged applications to an official account.

~~(CUI)~~ We determined that DISA offered more than [redacted] authorized unmanaged communication and messaging applications through its PUMA store for personal use on DoD mobile devices. However, the use of unmanaged messaging applications has not always been limited to personal use, which can result in violations of DoD electronic messaging and Federal and DoD records retention policies. For example, on March 31, 2021, the former DDS Director issued an authorization to operate that included an authorization to use [redacted] to discuss official DoD CUI information in violation of DoD electronic messaging policy prohibiting the use of unmanaged electronic messaging services for official DoD information.[19] The authorization required that users configure [redacted] to delete messages automatically [redacted], which violates the Federal and DoD records retention policy requirements to retain official DoD business for a minimum of 7 years.

(U) Recently, in response to a FOIA request for January 6, 2021 text messages, DoD officials disclosed that for DoD and Army officials "no longer with the agency, the text messages were not preserved." On January 12, 2021, a government oversight group submitted four FOIA requests to the DoD and the Army for all records of communications, including text messages

[17] (U) DoDI 8170.01 includes an exception that allows DoD Components to approve the use of non–DoD-controlled electronic messaging services by authorized users for public communications related to assigned duties, such as recruiting, or any other purpose deemed necessary and in the interest of the DoD. However, the Instruction states that use should be limited to supplemental communication only. The Instruction also states that DoD personnel may only use their personal, non-official messaging accounts for official DoD business in the case of an emergency, when other capabilities are not available, and use of the service is in the interests of the DoD.

[18] (U) DoDI 5015.02 references the exceptions listed in DoDI 8550.01, "DoD Internet Services and Internet-Base Capabilities," September 11, 2012 that was canceled and replaced by DoDI 8170.01. Footnote 17 describes the exceptions listed in DoDI 8170.01.

[19] ~~(CUI)~~ [redacted] is a text messaging, video, and voice-calling application for use on mobile devices. [redacted] secures messages, phone calls, and video calls with end-to-end encryption. End-to-end encryption means that content (for example, text, voice, video, and data) is encrypted all the way from sender to recipient without being readable to servers or other services along the way. Authorization to operate is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

(U) between DoD and Army officials and the White House on January 6, 2021.[20] The FOIA requests also asked that the DoD and Army take steps to ensure that records were not deleted before the request was processed. However, on March 10, 2022, the DoD and Army stated that the requested text messages were not preserved, but could have been saved in other records systems and explained that when an official leaves the agency, the official's DoD mobile device is erased.

(U) On August 3, 2022, after news reports that the DoD deleted the text messages, the Deputy Secretary of Defense issued a memorandum directing all mobile device service providers in the DoD to capture and save the data residing on DoD mobile devices that are turned in by personnel leaving the DoD.[21] However, while personnel are using their DoD mobile devices, the DoD cannot track or retain communications sent over unmanaged messaging applications. This poses the risk that DoD personnel may inadvertently lose, intentionally delete, or fail to preserve important DoD communications sent over these applications in violation of Federal and DoD records retention policies. It also creates the opportunity for DoD personnel to conceal communications and circumvent the creation of official DoD records, sheltering them from scrutiny or oversight.

(U) DoD Components and the DMUC Offered Users Unrestricted Access to Public Application Stores

~~(CUI)~~ DoD Components, including at least 26 Components that use the DMUC, offered DoD mobile device users unrestricted access to public applications stores, allowing personnel to download unauthorized unmanaged mobile applications to their DoD mobile devices.[22] Public application stores offer a wide variety of applications for mobile devices, such as games, news, travel, and messaging applications. These applications may include unnecessarily invasive permissions that require access to user contact lists and photos, and access to the device's sensors, such as the camera, microphone, or GPS. Unauthorized unmanaged applications may also contain malicious code. Components that use internal, non-DMUC mobile device management systems can restrict users' ability to install unauthorized unmanaged applications by creating [redacted] or application stores; or, by removing access to public application stores all together. However, the DoD Components that subscribe to the DMUC for mobile device management cannot restrict users' ability to install unauthorized unmanaged applications because the DMUC allows unrestricted access to public application stores, in accordance with the DoD CIO memorandum.

[20] (U) The DoD officials included the Acting Secretary of Defense, Chief of Staff to the Acting Secretary of Defense, and the General Counsel of the DoD. The Army officials included the Secretary of the Army, Chief of Staff to the Army, General Counsel of the Army, and Director of the Army Staff. The White House officials included the President of the United States, the Chief of Staff, the Vice President of the United States, the Chief of Staff to the Vice President, or anyone communicating on their behalf.

[21] (U) Deputy Secretary of Defense memorandum, "Records Management Responsibilities for Text Messages," August 3, 2022.

[22] (U) DoD comprises 46 Components. According to DISA officials, the DMUC manages approximately 140,000 DoD mobile devices for 130,000 DoD users.

~~(CUI)~~ We analyzed the mobile applications installed on [redacted] mobile devices, a Component that subscribes to the DMUC. Of the [redacted] unique applications installed on [redacted] mobile devices, approximately [redacted] were unauthorized unmanaged applications that were available only from public application stores.[23] The unauthorized unmanaged applications included approximately:

- ~~(CUI)~~ [redacted] entertainment applications, including video streaming, online radio, and fantasy football applications;
- ~~(CUI)~~ [redacted] personal applications, including online dating, real estate, and restaurant reservation applications;
- ~~(CUI)~~ [redacted] games, including children's games, puzzle games, and multiplayer online role-playing games;
- ~~(CUI)~~ [redacted] shopping applications, including online auction, consumer rewards, and luxury yacht dealer applications;
- ~~(CUI)~~ [redacted] electronic messaging applications, including applications with end-to-end encryption and automatic message deletion capabilities;
- ~~(CUI)~~ [redacted] cryptocurrency applications;
- ~~(CUI)~~ [redacted] personal business applications, including multi-level marketing, real estate showing manager, and payroll manager applications;
- ~~(CUI)~~ [redacted] third-party Virtual Private Network applications; and
- ~~(CUI)~~ [redacted] printer applications.[24]

~~(CUI)~~ Many of the unauthorized unmanaged applications required access to the camera, microphone, or GPS; examples included photo and video editing, telehealth, weather, maps, and fitness applications. In addition, some of the unauthorized unmanaged applications that [redacted] users downloaded to DoD devices had known cybersecurity risks, operational security risks, potentially inappropriate content, or represent unacceptable use of DoD mobile devices. For example, two of the applications downloaded were from a Chinese commercial off-the-shelf drone manufacturer that allow users to fly drones and capture, edit, and share images. On July 23, 2021, the DoD issued a press release stating that in 2018 the DoD issued a ban on the purchase and use of all commercial off-the-shelf drones, regardless of manufacturer, due to cybersecurity concerns.[25] The following year, Congress passed legislation specifically banning the purchase and use of drones and components

[23] ~~(CUI)~~ Approximately [redacted] applications did not appear on the DMUC's published lists of official and personal-use applications available for download through the DMUC's application stores as of March 21, 2022.

[24] (U) DoD CIO memorandum, "Authorized Telework Capabilities and Guidance," April 13, 2020, prohibits the connection of a personal printer to government-furnished equipment.

[25] ~~(CUI)~~ [redacted]

~~(CUI)~~ manufactured in China.[26] The downloading of applications used to fly Chinese commercial off-the-shelf drones onto DoD devices appears to be counter to DoD policy and could pose cybersecurity concerns.

(U) Examples of applications with potentially inappropriate content include applications for the creation of short-form videos; communication applications that have been exploited by violent extremists, hate groups, and sexual predators; and sexually themed games. Examples of applications that represent possible unacceptable use of DoD mobile devices include applications for live streaming crimes, police scanners, and gambling.

~~(CUI)~~ A [redacted] official expressed frustration with the DMUC services, specifically that the DMUC does not offer Components visibility into the mobile device data of their personnel.[27] The [redacted] official explained that Components must rely on DISA to run reports upon request, monitor the applications downloaded by users, and remove any applications that pose cybersecurity risks. This official stated that because the DMUC does not allow Components to run their own reports, [redacted] cannot readily monitor what applications its users are downloading or identify risky applications. The [redacted] official stated that Components must wait for DISA to determine that an application is an operational or cybersecurity risk and for DISA to identify the users who have downloaded the application.

(U) DoD Components Offered Users Mobile Applications Without Security Assessments

(U) The DoD CIO does not require DoD Components to conduct operational or cybersecurity assessments of unmanaged applications if the mobile devices meet requirements in the DoD CIO memorandum. The DoD CIO memorandum states that unmanaged applications will only be permitted on properly configured DoD mobile devices capable of segregating managed and unmanaged applications and their data.[28] The memorandum also requires users to sign a user agreement stating that they have received training regarding the operational security concerns of unmanaged applications. If DoD Components and users meet the memorandum's requirements, the DoD CIO does not require further evaluation of unmanaged applications before installation on DoD mobile devices. As a result, the DoD CIO allows users to have unrestricted access to unauthorized unmanaged applications from public application stores without security assessments.

---

[26] (U) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," Sec. 848, "Prohibition on Operation or Procurement of Foreign-Made Unmanned Aircraft Systems," December 20, 2019.

[27] ~~(CUI)~~ According to DISA officials, the DMUC mobile device management software allows DoD Component mobility administrators to see the applications installed on individual users' devices. The officials further stated that upon request from the DoD Component mobility administrators, DISA can provide a consolidated report of applications installed on all their users' devices. According to [redacted] officials, DoD Components that subscribe to the DMUC through another Component cannot directly access individual or consolidated installed application data for their mobile device users.

[28] (U) The DoD CIO memorandum states that Components must configure the devices to prevent unmanaged applications from accessing CUI, extracting CUI, or connecting to any systems that contain CUI.

(U) However, unmanaged applications pose a threat to the DoD through indirect access to DoD information or systems. For example, mobile device users can share official DoD information over unmanaged applications. In addition, many unmanaged applications routinely require access to a user's contact list, location data, and photo library that could reveal sensitive DoD locations and information. Unmanaged applications could also contain malicious code to record screen activity, log keystrokes, or activate the microphone posing a risk of cyber espionage.

(U) DISA acknowledges the risks that unmanaged applications pose to the DoD by presenting a banner warning to DMUC users on their mobile devices when downloading authorized unmanaged applications from the PUMA store. The banner warning states that the applications may compromise personal or U.S. Government data; may record video, take pictures, or record voice; may monitor the GPS and disclose sensitive locations; and may access the user's U.S. Government contacts and calendar resulting in disclosure of U.S. Government information. In addition, while DoDI 8170.01 and the DoD CIO Memorandum require DoD Components to provide mobile device and application training to mobile device users, the DoD does not offer training that covers all the topics required by DoDI 8170.01 and the DoD CIO memorandum.

(U) According to the DoD Security Technical Implementation Guides for Apple iOS and Android mobile devices, one way to prevent users from installing unauthorized unmanaged or malicious applications is to force users to install all applications from authorized application stores. DoD Components can create and control application stores to offer users only Component-selected applications. However, this is only an effective control if the Components assess the applications for security risks before including them in the application store.

~~(CUI)~~ For example, DISA has created several application stores for the DMUC users, including the DoD Apps and Managed Google Play stores for managed applications, and the PUMA store for unmanaged applications. As of April 11, 2022, we identified that DISA offered [redacted] managed applications and [redacted] authorized unmanaged applications through its application stores.

(U) DISA officials stated that while they do not conduct the same in-depth cybersecurity assessment for unmanaged applications as they do for managed applications, DISA does conduct a one-time security and risk assessment before authorizing unmanaged applications for the PUMA store. DISA officials stated that they also use security software installed on DMUC users' mobile devices to monitor for threats from unmanaged applications.

(U) However, we determined that DISA offered several authorized unmanaged applications through PUMA with known cybersecurity vulnerabilities including:

- (U) applications that accessed data saved to the clipboard of the operating system, which could include passwords, account-reset links, and personal messages, including popular weather and news applications; and

- (U) Android applications that were vulnerable to CVE-2020-8913, a vulnerability that allowed malicious code execution in popular applications, including messaging and social media applications.

~~(CUI)~~ Additionally, we identified approximately [redacted] authorized unmanaged applications offered through DISA's PUMA store that access GPS. In 2018, news outlets reported that the locations of sensitive DoD facilities and personnel had been publicly exposed through use of a fitness application. In response, the Deputy Secretary of Defense memorandum, "Use of Geolocation-Capable Devices, Applications, and Services," prohibited the use of geolocation features and functionality on both personal and DoD mobile devices, applications and services while in operational areas. The memorandum stated that for all other locations, the DoD Component heads will consider the inherent risks associated with geolocation capabilities on personal and DoD mobile devices used by personnel on and off duty. The memorandum further stated that when the capabilities pose a threat to personnel and operations, commanders and supervisors will provide operational security training and apply any restrictions consistently and rationally.

(U) DoD Components Lacked Controls over Personal Use of DoD Devices

~~(CUI)~~ DoD Components lacked controls over personal use of DoD mobile devices to ensure that personal use was limited, complied with DoD policies and regulations, and did not pose operational and cybersecurity threats to the DoD. DoD Regulation 5500.07-R states that DoD-owned communication systems and equipment (including mobile devices) should be for official use and authorized purposes only. We found that as of April 11, 2022, [redacted] percent of applications offered by the DMUC through its application stores were unmanaged applications for personal use on DoD mobile devices. At least one unmanaged application, [redacted], was used by DoD personnel in violation of DoD electronic messaging and record retention policies. Many of the unmanaged applications downloaded to DoD mobile devices have known operational and cybersecurity risks.

(U) The Director of DISA's Enterprise Integration and Innovation Center/CIO stated that DISA offers unmanaged applications through DMUC application stores to support DoD mission requirements. These applications include airline, hotel, and other travel applications for employees traveling on official DoD business; and, video, voice, or text messaging applications, to support DoD training. The Director also stated that DISA offers unmanaged applications to support the welfare of DoD personnel. DoD Regulation 5500.07-R provides an exception in the interest of morale and welfare, but only for military and civilian personnel on extended deployment and when approved by theater commanders. The unmanaged applications, as well as all the applications in the public application stores, are available to all DMUC users, regardless of deployment status.

~~(CUI)~~ DoD Regulation 5500.07-R provides a second exception for limited personal use of DoD devices when the use serves a legitimate public interest and does not reflect adversely on the DoD, among other requirements.[29] However, we identified unmanaged applications available through DISA's PUMA store that do not clearly fit the definition of legitimate public interest or may reflect adversely on the DoD because they violate a DoD policy or pose an operational or cybersecurity risk to the DoD, including more than:

- ~~(CUI)~~ [redacted] entertainment applications, including video streaming, golfing, and restaurant review applications;
- ~~(CUI)~~ [redacted] applications that access the camera, including live video broadcasting, shopping, and messaging applications;
- ~~(CUI)~~ [redacted] applications that access the microphone, including home security system, dictation, and walkie-talkie applications; and
- ~~(CUI)~~ [redacted] banking applications, including credit card payment, personal banking, and investment applications.

(U) We also analyzed how DoD Components request new applications from the DMUC. We identified that although DoD Components submitted application requests that indicated their intent to use the applications for official DoD business, DISA approved the applications as unmanaged for personal use. For example, two DoD Components requested authorization to use electronic messaging applications to save on the cost of international mission-related texts and calls. However, because the DoD Components stated on their requests that applications would not transmit CUI, DISA processed and approved the requests as unmanaged applications, even though the applications would be used for unclassified official DoD business. DISA officials stated that they would confirm the DoD Component's intended use of the application when there is a "very clear contradiction" in the request. However, DISA officials could not confirm whether they reviewed the intended use for the electronic messaging applications with the requesting Components.

(U) In these cases, DoD Components received a system-generated e-mail stating that the application had been approved for unmanaged use without a definition of "unmanaged use." As a result, the DoD Components may have believed that DISA approved the electronic messaging applications for official DoD business and used the applications in the manner stated on their requests.

[29] (U) DoD Regulation 5500.07-R defines legitimate public interest as keeping DoD employees at their desks rather than requiring the use of commercial systems; educating the DoD employee on the use of the communications system; enhancing the professional skills of the DoD employee; or job-searching in response to U.S. Government downsizing. Uses that would reflect adversely on the DoD include pornography; chain letters; unofficial advertising, soliciting, or selling, except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service.

(U) The DoD Lacks Mobile Device and Application Policy

(U) The DoD does not have a comprehensive mobile device and mobile application policy for Components and users. Instead, the DoD relies on a variety of policies, memorandums, Security Technical Implementation Guides, and user agreements that do not fully address the operational and cybersecurity risk that mobile device features or applications pose to DoD information and information systems. Without a common baseline of acceptable risk, Components' mobile device programs vary widely in the features and applications that users are permitted to access and use. As a result, the Components' mobile device programs also vary widely in the operational and cybersecurity risk they pose to the DoD.

(U) The existing DoD policies and guidance use different terminology to refer to applications for official DoD business, including "approved," "managed," "DoD-controlled," "authorized," and "official." For example, DoD CIO memorandum, "Mobile Application Security Requirements," defines managed and unmanaged applications, but does not make clear that managed applications are approved, DoD-controlled, and official applications for DoD business official. Additionally, DoDI 5015.02 refers to official and non-official electronic messaging accounts, while DoDI 8170.01 refers to DoD-controlled and non–DoD-controlled electronic messaging services. Because users do not receive adequate training to identify the difference between managed and unmanaged applications, DISA's list of authorized applications can be misinterpreted to mean that unmanaged, personal-use applications from the PUMA store are authorized for official DoD business.

(U) The DoD's mobile device and application training is inadequate, does not meet the policy requirements, and is not required annually. DoD CIO memorandum, "Mobile Application Security Requirements," requires DoD Component heads to provide training on the "operational security concerns introduced by unmanaged applications including applications utilizing GPS tracking and other non-cybersecurity and/or privacy related concerns" to mobile device users. In addition, DoDI 8170.01 requires DoD Components to provide training on the responsible and effective use of electronic messaging services as well as cybersecurity, operational security, and records management, among other topics.

(U) Because the DoD lacks comprehensive mobile device policy, Components determine the content of and how often their users receive training on the acceptable use of their mobile devices and applications. The DoD does offer training for mobile device users, including, the DoD Cyber Awareness Challenge, Government Ethics training, and Using Mobile Devices in a DoD Environment, in addition to mobile device user agreements. However, the existing DoD training does not teach users:

- (U) the difference between managed, authorized unmanaged, and unauthorized unmanaged applications;
- (U) how to identify applications approved for official DoD business, including which applications are approved for unclassified and CUI communications;

- (U) the operational and cybersecurity risks posed by authorized unmanaged applications from application stores and unauthorized unmanaged applications from public application stores;
- (U) the operational and cybersecurity risks posed by mobile device features such as GPS, microphone, and screen capture;
- (U) how to protect sensitive DoD information on mobile devices;
- (U) how to comply with records management requirements; and
- (U) the acceptable uses of DoD mobile devices.

(U) As a result, the DoD Components can manage mobile device programs in different ways. For example, the Defense Logistics Agency's (DLA) mobile device program is highly restrictive. The DLA's mobile device management policy requires the disabling of GPS, screen capture, electronic messaging (other than DLA-approved and hosted services), and access to public application stores.[30] It also prohibits the use of the camera and video messaging, among other features, unless approved for use. The policy states that the DLA must complete a risk assessment and approve all mobile applications before deployment. The DLA Mobile Device User Agreement states that mobile devices are for official government use only with limited exceptions. By restricting users' access to some mobile device features and public application stores, the DLA has reduced the risk that users will inadvertently share sensitive DoD information or introduce malware to DoD information systems.

(U) In contrast, the DMUC program is highly permissive and allows mobile device users to have access to GPS, screen capture, and camera features. DMUC users also have unrestricted access to public application stores and can install almost any application they choose. The DMUC also initially configures users' DoD mobile devices to enable geolocation services and makes the users responsible for turning off geolocation services.

(U) In addition, DISA permits users to use their DoD mobile devices for personal activities and offers unmanaged applications through its PUMA application store. By permitting users to access nearly all mobile device features and applications, DISA has increased the risk that users will misuse or abuse their DoD mobile devices and increased the operational and cybersecurity risk to DoD information and information systems.

(U) Operational and Cybersecurity Risk to the DoD

(U) The DoD's inadequate controls over the use of mobile applications poses an operational and cybersecurity risk to DoD information and DoD information systems. DoD Components' mobile application programs, including DISA's DMUC, that allow users broad access to mobile device features and unmanaged applications increase the risk that users will violate Federal and DoD policies, including records retention policies, inadvertently reveal sensitive DoD information, or introduce malware to DoD information systems.

[30] (U) DLA Instruction 8130.01, "Mobile Device Management," September 27, 2013.

(U) DISA and other DoD Components that allow their personnel unrestricted access to public application stores, and DISA's lack of controls over public application stores increase the risk that personnel will download compromised applications that can expose DoD information or introduce malware to DoD systems. DISA and other DoD Components that manage their own mobile devices must configure their mobile devices to segregate unmanaged applications to prevent them from accessing DoD CUI data or systems. However, the applications, or malware, can evade that protection by accessing the microphone to eavesdrop, recording screen activity when the user accesses DoD data or systems, collecting location data of DoD personnel, or other malicious activity.

(U) According to a cybersecurity company's research, most malware is downloaded from public application stores; however, malicious actors have increasingly used text and mobile messaging to deliver malware to mobile devices. Malware can steal sensitive information such as banking credentials, financial data, login credentials, contact lists, e-mails, and text messages. The National Information Assurance Partnership warns that malware may also attack a device's platform software to gain additional privileges and the ability to conduct further malicious attacks.[31]

(U) The malware may be able to control features on the device, such as GPS, camera, or microphone, to gather intelligence by tracking users' locations, recording telephone calls and video, or eavesdropping on users' surroundings. The National Information Assurance Partnership also states that malware may provide access to network systems to conduct network-based attacks.

(U) For example, a recent report from a global online cybersecurity company found that malware and malicious links were spread through fake coronavirus disease–2019 vaccine registration applications, text messages, and social media messages. The malware displays unwanted advertisements, forwards itself to the user's contacts, and takes full control of the device. The company also found an increase in banking Trojan malware spread through text messages and applications from a public application store. The banking Trojans mimic legitimate banking and financial applications to not only steal banking credentials, but also disable the security functionality, take full control of the device, monitor keystrokes, record the screen, conduct covert surveillance, and intercept communications. In another example, a vulnerability in an electronic messaging application allowed malicious actors to install spyware onto mobile devices. The spyware was able to activate the microphone and camera, read e-mails and messages, and collect location data.

[31] (U) The National Information Assurance Partnership is a program managed by the National Security Agency to evaluate commercial off-the-shelf information technology products for conformance to international security requirements. National Information Assurance Partnership, "Mobile Device Fundamentals, Version 3.2," April 15, 2021, available at https://www.niap-ccevs.org/MMO/PP/PP_MDF_V3.2.pdf.

(U) Many seemingly harmless commercial applications also pose a threat to DoD information and information systems when they require unnecessarily invasive permissions on DoD mobile devices. Video games, shopping, or weather applications routinely require access to a device's contact list, messaging platforms, location data, or other personal information, and often lack sufficient security or encryption standards. In 2021, a software company published a study of 100,000 popular applications that found that mobile applications regularly request access to features that are seemingly unrelated to their functionality. For example, the study found that:

- (U) 83 percent of shopping applications requested access to the camera;
- (U) 62 percent of news applications requested access to the photo library;
- (U) 56 percent of games requested access to the calendar;
- (U) 53 percent of sports applications requested access to location; and
- (U) 40 percent of entertainment applications requested access to the microphone.

(U) In addition, DoD users can easily transmit official DoD information, including CUI, over unmanaged applications, increasing the risk of exposing sensitive information, negatively impacting DoD missions, and violating records retention requirements. While unmanaged applications cannot technologically access CUI on the mobile device, there are no controls to prevent users from discussing or sharing CUI over unmanaged applications. This is especially true when DoD Components allow the use of screen capture or copy and paste functionality on the mobile device. By allowing DoD users to have broad access to mobile device features and unmanaged applications, the DoD is increasing the risk of compromise of DoD data and information systems.

(U) Management Comments on the Background and Finding and Our Response

(U) Revised Appendixes

(U) We made the decision to remove Appendixes A, B, and C that contained listings of the mobile applications offered to or installed by DoD Components due to operational security concerns identified by DoD Components during their security reviews.

(U) The DISA CIO provided the following comments on the background and finding. For the full text of the DISA CIO's comments, see the Management Comments section of the management advisory.

(U) Defense Information Systems Agency Comments on the Background

(U) The DISA CIO stated that the DoD Mobile Application Store and PUMA store are gateways to obtaining products through public application stores. He explained that the user agreement states that users should only download approved unmanaged applications from the PUMA store. The DISA CIO also stated that while some types of mobile devices are restricted to only loading applications listed in the DoD application stores, other types of mobile devices allow users to download any application in the public application store. Finally, the DISA CIO stated that when DISA receives a request for applications to be added to a DoD application store, DISA officials perform a security assessment and make a risk determination for the application.

(U) Our Response

(U) We acknowledge that the DoD application stores contain links to where the managed and authorized unmanaged applications are available for download from the public application stores. Although the various versions of the user agreements we reviewed stated that downloading unauthorized applications may result in the device being flagged, the agreements do not state that users should only download applications from the DoD stores. We acknowledge that DISA conducts a one-time security and risk assessment before authorizing unmanaged applications for the PUMA store, and discuss this process in this advisory in the section titled, "DoD Components Offered Users Mobile Applications Without Security Assessments."

(U) Defense Information Systems Agency Comments on the Finding

(U) The DISA CIO stated that DISA provides organizations that subscribe to the DMUC with a user agreement that outlines the conditions for the secure and appropriate use of a mobile device. The DISA CIO stated that DoD policy requires DoD personnel to complete cyber awareness training annually, which addresses many cyber hygiene-related issues, while the Components using the DMUC service are responsible for any remaining training needs. In addition, he explained that depending on the manufacturer, some mobile devices

(U) allow users to readily identify managed from unmanaged applications. To assist users of mobile devices without this capability, DISA provides listings of the managed and unmanaged applications on the DMUC Mobility Portal website.

(U) Our Response

(U) We agree that DoD mobile device users are required to take training; however, the training lacks important content. Specifically, as discussed in this management advisory in the third paragraph of the section titled, "The DoD Lacks Mobile Device and Application Policy," the training that the users receive lacks instruction on the difference between and how to identify managed and unmanaged applications. Because of this, users could misidentify unmanaged applications as authorized for official DoD business.

(U) Recommendations, Management Comments, and Our Response

(U) Revised, Redirected, and Renumbered Recommendations

(U) As a result of management comments, we revised and consolidated Recommendations 2 and 3 to recommend the DoD CIO develop policy requiring DoD Components to justify and approve the mission requirements for managed and unmanaged applications and limit access to only justified applications. We also redirected Recommendation 5 from the Director of Defense Digital Services to the Director of the Chief Digital and Artificial Intelligence Office Directorate for Digital Services, to reflect the Director's new title after the integration of the Defense Digital Services into the DoD Chief Digital and Artificial Intelligence Office. We also renumbered draft Recommendation 4 as Recommendation 3, Recommendation 5 as Recommendation 4, and Recommendation 6 as Recommendation 5.

(U) We revised Recommendations 1.d, 3, and 4.c to require that the DoD establish or revise policy to address the recommendations, which was implied but not directly stated in the draft recommendations.

(U) Recommendation 1

(U) We recommend that the DoD Chief Information Officer direct the DoD Components to immediately:

a. **(U) Require users to forward a complete copy of all official DoD messages generated over unmanaged electronic messaging applications to an official electronic messaging account.**

b. **(U) After completion of Recommendation 1.a, remove all unauthorized unmanaged applications from all DoD mobile devices.**

c. **(U) After completion of Recommendation 1.a, assess all unmanaged applications for operational and cybersecurity risks and remove those with unacceptable risks or without a justifiable need from users mobile devices and Component application stores.**

d. **(U) Assess mobile device users' access to public application stores and remove access of those without a justifiable need. If unable to remove mobile device users' access, require Components to develop and implement policy that defines the acceptable use of public application stores and requires periodic assessments of mobile device users downloads to determine that all applications have a justifiable need.**

(U) DoD Chief Information Officer Comments

(U) The DoD CIO agreed, stating that he will provide the detailed corrective actions for the recommendations once the DoD develops a plan to address the Deputy Secretary of Defense's approved courses of action related to records management for text messaging.

(U) Our Response

(U) Although the DoD CIO agreed with the recommendations, we cannot resolve the recommendations until we can determine whether the corrective actions will meet the intent of the recommendations. Therefore, the recommendations are unresolved, and we request that the DoD CIO provide the detailed corrective actions once the DoD develops a plan to address the Deputy Secretary of Defense's courses of action for records management.

(U) Recommendation 2

(U) We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Intelligence and Security, develop comprehensive mobile device and mobile application policy for Components and users. The policy should, at a minimum:

- **a. (U) Define the acceptable use of DoD mobile devices and mobile applications for official DoD business and personal use.**
- **b. (U) Address the cybersecurity and operational security risks of:**
  1. **(U) User access to unmanaged applications without cybersecurity assessments through Component application stores or public application stores.**
  2. **(U) Mobile device features, including geolocation, screen capture, copy and paste, and camera, among others.**
- **c. (U) Address the DoD records management requirements of DoD Instruction 5015.02, "DoD Records Management Program," February 25, 2015 (Incorporating Change 1, August 17, 2017) and the Deputy Secretary of Defense memorandum "Records Management Responsibilities for Text Messages," August 3, 2022.**
- **d. (U) Require DoD Components to provide regularly scheduled training to DoD mobile device users on the responsible and effective use of mobile devices and applications, including electronic messaging services, in accordance with DoD Chief Information Officer memorandum, "Mobile Application Security Requirements," October 6, 2017, and DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019 (Incorporating Change 1, August 24, 2021). The training should address, at a minimum:**
  1. **(U) Ethics guidelines to ensure compliance with DoD 5500.07-R, "Joint Ethics Regulation," August 30, 1993 (Incorporating Change 7, November 17, 2011).**
  2. **(U) Definitions of, difference between, and responsible use of managed and unmanaged applications on DoD mobile devices.**
  3. **(U) Best practices when using unmanaged applications.**
  4. **(U) Operational security concerns, potential threats, and risks associated with using unmanaged applications, which may contain capabilities such as location sharing (GPS tracking), personal information sharing, or may have nefarious characteristics (for example, marketing scams, and human trafficking).**
  5. **(U) Cybersecurity concerns associated with using unmanaged applications, which may contain malware or spyware.**
  6. **(U) Privacy-related concerns.**

7. **(U) Records management requirements to ensure compliance with DoD Instruction 5015.02, "DoD Records Management Program," February 25, 2015 (Incorporating Change 1, August 17, 2017).**
8. **(U) Information review for clearance and release authorization procedures.**
9. **(U) Accessibility standards to ensure compliance with DoD Manual 8400.01, "Accessibility of Information and Communications Technology," November 14, 2017.**

e. (U) Require DoD Components to justify and approve the mission requirements for all managed and unmanaged applications and limit access to only those applications with a justified and approved need.

(U) DoD Chief Information Officer Comments

(U) The DoD CIO agreed, stating that he has written a draft memorandum, "Use of Mobile Applications in the Department of Defense," to address the operational security risk posed by the unapproved use of mobile applications that may result in the unauthorized disclosure of DoD information. In addition, the DoD CIO stated that he will provide the detailed corrective actions for the recommendations once the DoD develops a plan to address the Deputy Secretary of Defense's approved courses of action related to the records management for text messaging.

(U) Our Response

(U) Comments from the DoD CIO did not address the specifics of the recommendations; therefore, the recommendations are unresolved. We disagree that the DoD CIO's draft memorandum comprehensively addresses the operational security risk posed by the unapproved use of mobile applications. Instead, the draft memorandum references elements of existing DoD mobile device and application policies. As noted in this management advisory, we identified that the DoD already relies on a variety of policies, memorandums, Security Technical Implementation Guides, and user agreements that do not address the operational and cybersecurity risk that mobile device features or applications pose to DoD information and information systems. The draft memorandum does not define the acceptable use of DoD mobile devices and mobile applications for official DoD business and personal use (Recommendation 2.a) and does not fully address the cybersecurity and operational security risks of unmanaged applications (Recommendation 2.b.1) and mobile device features (Recommendation 2.b.2).

(U) In addition, the draft memorandum does not address how Components and users can comply with DoD Records Management policies when using mobile applications (Recommendation 2.c). Furthermore, it does not address the DoD's training requirements (Recommendation 2.d). Therefore, we request that the DoD CIO, in coordination with the Office of the Under Secretary of Defense for Intelligence and Security (OUSD[I&S]), provide

(U) comments on the final management advisory addressing the need for the development of a comprehensive mobile device and mobile application policy for Components and users that fully addresses each element of the recommendations.

(U) Although the DoD CIO also agreed with draft management advisory Recommendation 3, we revised and renumbered that recommendation as Recommendation 2.e. Therefore, we request that the DoD CIO provide comments on the final management advisory Recommendation 2.e.

(U) Under Secretary of Defense for Intelligence and Security Comments

(U) The Acting Director for Defense Intelligence, Counterintelligence, Law Enforcement, and Security, responding for the Under Secretary of Defense for Intelligence and Security, agreed, stating that the OUSD(I&S) will coordinate comprehensive mobile device and mobile application policy for Components and users to be developed by the DoD CIO. The Acting Director added that the OUSD(I&S) issued memorandum, "Information and Operations Security Risks Posed by Non-Government Websites and Applications," June 22, 2021, which also addresses the recommendations. Finally, the Acting Director added that, as the primary action office, the DoD CIO would provide a response to the recommendations.

(U) Our Response

~~(CUI)~~ Comments from the Acting Director did not address the specifics of the recommendations; therefore, the recommendations are unresolved. The OUSD(I&S) memorandum [redacted] however, it does not provide guidance on the acceptable use of mobile devices and mobile applications. We request that the DoD CIO, in coordination with the OUSD(I&S), develop a comprehensive mobile device and mobile application policy for Components and users that fully addresses each element of the recommendation.

(U) Defense Information Systems Agency Comments

(U) Although not required to comment, the DISA CIO stated that DISA cannot restrict applications per user. He explained that if an application is approved for one user, it will be available for all users. The DISA CIO also stated that DISA should not determine whether mobile applications support a mission related requirement. The DISA CIO suggested that the recommendation be revised to recommend that the DoD CIO develop policy requiring DoD Components to justify and approve the mission requirements for all managed and unmanaged applications and limit access to only those appropriately justified applications.

(U) Our Response

(U) Comments from the DISA CIO clarified DISA's ability to restrict individual users' access to mobile applications. As a result, we revised and consolidated Recommendations 2 and 3 to require the DoD CIO to develop policy requiring DoD Components to justify and approve the mission requirements for all managed and unmanaged applications and limit access to only those appropriately justified applications.

(U) Recommendation 3

(U) We recommend that the DoD Chief Information Officer, in coordination with the Defense Information Systems Agency Chief Information Officer, revise DoD policy and memorandums and Defense Information Systems Agency mobile application documentation and training to ensure the use of common terminology when referring to approved, managed, DoD-controlled, authorized, and official applications; and unmanaged, non–DoD-controlled, unauthorized, non-official, and personal-use applications.

(U) DoD Chief Information Officer Comments

(U) The DoD CIO agreed, stating that he will provide the detailed corrective actions for the recommendation once the DoD develops a plan to address the Deputy Secretary of Defense's approved courses of action related to the records management for text messaging.

(U) Our Response

(U) Although the DoD CIO agreed with the recommendation, we cannot resolve the recommendation until we can determine whether the corrective actions will meet the intent of the recommendation. Therefore, the recommendation is unresolved, and we request that the DoD CIO provide the detailed corrective actions once the DoD develops a plan to address the Deputy Secretary of Defense's courses of action for records management.

(U) Recommendation 4

(U) We recommend that the Defense Information Systems Agency Chief Information Officer:

a. **(U) Update the DoD Mobility Unclassified Capability service to provide Component mobile device managers reports and data regularly, at least quarterly, of the mobile applications downloaded to the mobile devices within the manager's area of responsibility.**

(U) Management Comments Required

(U) The DISA CIO did not provide comments on the recommendation; therefore, the recommendation is unresolved. We request that the DISA CIO provide comments on the final management advisory.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the DoD CIO agreed with the recommendation.

b. (U) Publish a clear list of applications approved for official DoD business and make the list easily accessible from DoD mobile devices.

(U) Defense Information Systems Agency Comments

(U) The DISA CIO partially agreed, stating that DISA publishes a list of the applications approved for official business on the DMUC mobility portal. The DISA CIO also stated that DISA would review options to make the list of applications more accessible to mobile device users.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the DoD CIO agreed with the recommendation.

(U) Our Response

(U) Comments from the DISA CIO addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the DISA CIO provides documentation showing that the list is easily accessible from DoD mobile devices.

c. (U) Develop and implement policy to conduct periodic reviews, at least annually, of the list of authorized unmanaged applications and remove those without a justifiable need or with known cybersecurity risks.

(U) Defense Information Systems Agency Comments

(U) The DISA CIO disagreed and suggested that the recommendation be removed. The DISA CIO stated that DISA does an initial assessment of an application before placing it in a DoD application store, which is more than what the DoD requires DISA to do. The DISA CIO also stated that because commercial mobile device managers cannot remove unmanaged applications from mobile devices, DISA instead uses supplemental mobile threat protection.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the DoD CIO agreed with the recommendation.

(U) Our Response

(U) Comments from the DISA CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. Although we acknowledge that DISA assesses applications before adding them to the application stores, DISA does not have a process to periodically review the list of authorized unmanaged applications and remove those applications from the list that do not have a justifiable need, have known cybersecurity risks, or are banned by the DoD. We request that the DISA CIO provide specific actions that DISA will take to conduct periodic reviews of and update the list of authorized unmanaged applications.

d. (U) Remove or hide any unauthorized unmanaged applications from the mobile devices of users who cannot demonstrate a justifiable need for the application.

(U) Defense Information Systems Agency Comments

(U) The DISA CIO disagreed and suggested that the recommendation be removed. The DISA CIO stated that because commercial mobile device managers cannot remove unmanaged applications from mobile devices, DISA instead uses supplemental mobile threat protection. The DISA CIO also stated that DISA cannot be held responsible for actions related to the business justification of mobile applications.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the DoD CIO agreed with the recommendation.

(U) Our Response

(U) Comments from the DISA CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. We acknowledge that mobile device managers cannot remove unmanaged applications; however, this recommendation does not require DISA to remove unmanaged applications using a mobile device manager. The intent of the recommendation is for DISA to limit users' access to unauthorized applications on the mobile devices because those applications cannot be used to conduct official DoD business or for personal use on DoD mobile devices. Therefore, if there is not a justifiable need for the mobile device user to access an unauthorized application, DISA must take action to prevent the user from accessing it. We request that the DISA CIO provide specific actions that DISA personnel will take to limit mobile device users' access to unauthorized unmanaged applications on DoD mobile devices.

e. **(U) Revise the "New Application Request" form to ask whether the Component intends to use the application to conduct official DoD business and processes requests that have the answer "Yes" to this question as managed applications.**

(U) Defense Information Systems Agency Comments

(U) The DISA CIO disagreed and suggested that the recommendation be removed. The DISA CIO stated that DISA's processes are aligned with the policies established by the DoD CIO, and therefore DISA should not be responsible for reviewing the business justification for the requested mobile applications. The DISA CIO also stated that many mobile application requests are for applications that may be used for official DoD business, such as vendor travel applications. However, he explained that those applications should not be categorized as managed because the applications could potentially have access to DoD CUI.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the DoD CIO agreed with the recommendation.

(U) Our Response

(U) Comments from the DISA CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The intent of the recommendation is to ensure that DISA conducts assessments on all mobile applications used for DoD official business to protect DoD information. We request that the DISA CIO provide specific actions DISA officials will to take to assess all mobile applications used for DoD official business.

(U) Recommendation 5

~~(CUI)~~ We recommend that the Director of the Chief Digital and Artificial Intelligence Office Directorate for Digital Services and associated activities cease and desist the use by the Directorate for Digital Services personnel of [redacted] and any other unmanaged applications to conduct official business and forward any available records from [redacted] to an official messaging account.

(U) Chief Digital and Artificial Intelligence Office Directorate for Digital Services Comments

~~(CUI)~~ The Chief Digital and Artificial Intelligence Office Directorate for Digital Services Director disagreed that DDS personnel had been authorized to use [redacted] or other unmanaged applications for official business, but she agreed with the balance of the recommendation. The Director stated that she would withdraw the referenced authorization issued by the former director, and inform the organization that requested the authorization of the withdrawal. The Director also stated that she would issue a memorandum reminding DDS employees that official business should not be conducted using [redacted] or any other unmanaged application and to forward any available records to official messaging accounts by October 31, 2022.

(U) DoD Chief Information Officer Comments

(U) Although not required to comment, the DoD CIO agreed with the recommendation.

(U) Our Response

(U) Comments from the Director addressed the specifics of the recommendation; therefore, the recommendation is resolved but open. On November 21, 2022, the Director issued a memorandum immediately withdrawing the referenced authorization issued by the former DDS Director and provided documentation demonstrating that the organization that requested the authorization was informed of the withdrawal. We will close the recommendation once the Director provides documentation showing that she issued the memorandum to DDS personnel reinforcing DoD policies regarding the use of unmanaged applications and records retention with an updated deadline for forwarding any available records to official messaging accounts.

(U) Management Comments

(U) Office of the Under Secretary of Defense for Intelligence and Security

~~CUI~~
UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENT

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE
AND SECURITY

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Management Advisory on the DoD's Use of Mobile Applications: Project No. D2021-D000CU-0143.001

On behalf of the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), I appreciate your team evaluating whether Department of Defense (DoD) personnel are conducting official business on DoD-issued mobile devices using mobile applications in such a way that poses operations security (OPSEC) risks by inadvertently revealing DoD critical information. Although OUSD(I&S) is not the primary office responsible for the oversight of policies related to the use of DoD-issued mobile devices, or mobile applications on those devices, OUSD(I&S) has partnered with the Office of the DoD Chief Information Officer (DoD CIO) due to those OPSEC risks. To the extent that OUSD(I&S) is a coordinating office on the recommendation, we concur with the draft management advisory recommendation that the OUSD(I&S) coordinate comprehensive mobile device and mobile application policy for Components and users to be developed by DoD CIO. As the primary action office, DoD CIO will respond for the recommendation itself.

OUSD(I&S) recommends the report remain marked "controlled unclassified information" (CUI) for OPSEC reasons. We assess that page 7 paragraph 2, page 9 paragraphs 1 and 2, page 12 paragraph 3, page 13 paragraph 2, page 14 paragraph 1, and the three appendixes contain CUI. To resolve these OPSEC concerns and allow public release, we suggest removing all [redacted] not identifying specific [redacted] not using [redacted] of various applications or downloads, and removing the appendixes. These changes effectively sanitize the document to make it unclassified.

Additionally, the draft management advisory requested OUSD(I&S) identify other actions taken to address the recommendations. OUSD(I&S) would like to highlight the attached OUSD(I&S) memorandum, "Information and Operations Security Risks Posed by Non-Government Websites and Applications," signed on June 22, 2021. My point of contact for this matter is [redacted]

DIXSON JOHN [redacted]

John P. Dixson
Acting Director for Defense Intelligence,
Counterintelligence, Law Enforcement,
& Security

Attachment: As stated

~~Controlled by: OUSD(I&S)/(CL&S)/PITY-OPSEC~~
~~CUI Category: OPSEC~~
~~Dissemination Control: FEDCON~~
~~POC:~~ [redacted]

~~CUI~~
UNCLASSIFIED WHEN SEPARATED FROM ATTACHMENT

(U) Office of the DoD Chief Information Officer

~~CUI~~

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

NOV 2 8 2022

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: (U) Review and Comment of DoD Inspector General "Management Advisory on the DoD's Use of Mobile Applications (Project No. D2021-D000CU-0143.001)

(U) This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Report, Management Advisory on the DoD's Use of Mobile Applications (Project No. D2021-D000CU-0143.001)

(U) DoD IG RECOMMENDATION 1.a-d: We recommend that the DoD Chief Information Officer direct the DoD Components to immediately:

a. Require users to forward a complete copy of all official DoD messages generated over unmanaged electronic messaging applications to an official electronic messaging account.

b. After completion of Recommendation 1.a, remove all unauthorized unmanaged applications from all DoD mobile devices.

c. After completion of Recommendation 1.a, assess all unmanaged applications for operational and cybersecurity risks and remove those with unacceptable risks or without a justifiable need from users mobile devices and Component application stores.

d. Assess mobile device users' access to public application stores and remove access of those without a justifiable need. If unable to remove mobile device users access, require Components to establish the acceptable use of public application stores and periodically assess mobile device users downloads to determine that all applications have a justifiable need.

(U) DoD CIO RESPONSE: DoD CIO agrees with the DoD IG recommendation.

~~Controlled by: Audit~~
~~Category: PRIVILEGE, OPERATIONAL SECURITY INFORMATION~~
~~LDC: FEDCON~~
~~POC: CSO Program Director,~~ [redacted]

~~CUI~~

(U) Office of the DoD Chief Information Officer (cont'd)

(U) DoD IG RECOMMENDATION 2: We recommend that the DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Intelligence and Security, develop comprehensive mobile device and mobile application policy for Components and users.

(U) DoD CIO RESPONSE 2: DoD CIO agrees with the DoD IG recommendation. Prior to the release of this IG advisory, The DoD CIO has the "Use of Mobile Applications in Department of Defense" memo in draft to address the unapproved use of mobile apps poses an operations security (OPSEC) risk and may result in the unauthorized disclosure of DoD information and jeopardize operations, strategies, or missions.

(U) DoD IG RECOMMENDATION 3: We recommend that the DoD Chief Information Officer direct DoD Component Heads and the Defense Information Systems Agency Chief Information Officer to limit the distribution of unmanaged applications to those users who can demonstrate a justifiable need for the application.

Revised and renumbered draft Recommendation 3 as Recommendation 2.e

(U) DoD CIO RESPONSE 3: DoD CIO agrees with the DoD IG recommendation.

(U) DoD IG RECOMMENDATION 4: We recommend that the DoD Chief Information Officer, in coordination with the Defense Information Systems Agency Chief Information Officer, use common terminology among DoD policy and memorandums and Defense Information Systems Agency mobile application documentation and training when referring to approved, managed, DoD-controlled, authorized, and official applications; and unmanaged, non–DoD-controlled, unauthorized, non-official, and personal-use applications.

Renumbered as Recommendation 3

(U) DoD CIO RESPONSE 4: DoD CIO agrees with the DoD IG recommendation.

(U) DoD IG RECOMMENDATION 5: We recommend that the Defense Information Systems Agency Chief Information Officer:

Renumbered as Recommendation 4

a. Update the DoD Mobility Unclassified Capability service to provide Component mobile device managers reports and data regularly, at least quarterly, of the mobile applications downloaded to the mobile devices within the manager's area of responsibility.
Concur. Providing quarterly reports and/or give Component mobile device managers access to reports with UEM systems.

b. Publish a clear list of applications approved for official DoD business and make the list easily accessible from DoD mobile devices.

c. Conduct periodic reviews, at least annually, of the list of authorized unmanaged applications and remove those without a justifiable need or with known cybersecurity risks.

d. Remove or hide any unauthorized unmanaged applications from the mobile devices of users who cannot demonstrate a

2

~~CUI~~

(U) Office of the DoD Chief Information Officer (cont'd)

justifiable need for the application.

e. Revise the "New Application Request" form to ask whether the Component intends to use the application to conduct official DoD business and processes requests that answer "Yes" to this question as managed applications.

(U) DoD CIO RESPONSE 5: DoD CIO agrees with the DoD IG recommendation.

Redirected and renumbered as Recommendation 5

~~(CUI)~~ DoD IG RECOMMENDATION 6: We recommend that the Director of the Defense Digital Service and associated activities cease and desist the use by Defense Digital Service personnel of [redacted] and any other unmanaged applications to conduct official business and forward any available records from [redacted] to an official messaging account.

(U) DoD CIO RESPONSE 6: DoD CIO agrees with the DoD IG recommendation.

(U) While the DoD CIO agrees with all recommendations, as discussed with the DoDIG, DoD CIO will address corrective actions for each recommendation in detail after publication of the Final Management Advisory and not until a detailed plan to address the Deputy Secretary of Defense's approved courses of actions related to the records management for text messaging is developed. The DoD CIO is currently coordinating with key stakeholders to address the recommendations of the management advisory and will keep the DoDIG informed on the status.

(U) The point of contact for this matter is [redacted]

John B. Sherman

3

~~CUI~~

(U) Defense Information Systems Agency

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

November 3, 2022

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

SUBJECT: Response to DoD IG Draft Management Advisory Project No. D2021-D000CU-0143.001 draft report, 3 October 2022

Reference: U.S. Department of Defense Inspector General's draft report "Management Advisory on the DoD's Use of Mobile Applications (Project No. D2021-D000CU-0143.001) 3 October 2022

The Defense Information Systems Agency (DISA) has reviewed the referenced draft advisory report and is providing specific clarification comments regarding information we believe is missing or not conveyed accurately in the report. In addition, DISA non-concurs with recommendations three and five as written as noted below.

General Report Comments:

Page 2 - IG Statement: *DOD Components that subscribe to the DMUC do not have direct control over their user's access to mobile applications. DISA operates the DMUC service and provides DMUC users with unrestricted access to public application stores, as well as access to the DMUC application stores, such as the DoD Mobile Application Store and Personal User Mobile Application (PUMA) store. DISA includes applications in the DMUC application stores after receiving a request for the application from a DoD component and assessing the application for cybersecurity risks. According to DISA's Enterprise Integration and Innovation Center Director/ Chief Information Officer (CIO), DISA can remotely remove managed mobile applications from user's devices and hide unmanaged applications from users through the DMUC. The DISA CIO also stated that for unmanaged applications, DoD components can only request that users remove the applications from their devices. However, the DISA CIO stated that DoD components can indirectly control user's access to mobile applications through component-level mobile application policy, user training, and reports of user's downloaded mobile applications.*

DISA Comment(s): DISA wishes to note that the DoD Mobile Application Storage and Personal Use Mobile Application (PUMA) store are essentially gateways to obtaining products through the vendor public application stores. Android devices are restricted to only loading applications listed in the DoD stores. Architectural issues with iOS systems previously prevented the use of a [redacted] combination, which ultimately allowed a user to download any application in the public app store. Such actions are viewed as a violation of the user agreement which clearly states that only approved unmanaged applications are to be loaded via the PUMA store.

(U) Defense Information Systems Agency (cont'd)

SUBJECT: Defense Information Systems Agency's (DISA) response to the U.S. Department of Defense Inspector General's draft report "Management Advisory on the DoD's Use of Mobile Applications (Project No. D2021-D000CU-0143.001) 3 October 2022

Page 3 – IG Statement: *Although the DoD Components, including DISA, are not required to conduct a cybersecurity assessment or review existing assessments of unmanaged applications, the authorizing official must assume the cybersecurity risks of allowing unmanaged applications to be installed on DoD mobile devices. In addition, the users must sign a user agreement acknowledging that they received training on the operational security risks introduced by unmanaged applications, including applications that use the global positioning system (GPS).*

DISA Comment(s): As noted in previous comment submissions, when DISA receives requests from DoD components for applications to be added to a DoD application store, a security assessment is performed, and a risk determination made prior to it be added to the DoD store. This important consideration is being noted for factual completeness.

Page 6 – IG Statement: *In addition, DISA and other DoD Components do not provide adequate training on the acceptable use of DoD mobile devices or applications. Contributing to the issue, DoD mobile device users cannot easily identify which of the mobile applications on their DoD mobile devices have been approved for DoD business.*

DISA Comment(s): DISA provides DMUC organizations with a user agreement which provides conditions for secure and appropriate use of a device. Per DoD policy, all DoD personnel are required to complete annual cybersecurity awareness training which addresses many cyber hygiene related issues. Additional training needs are the responsibility of the components leveraging DISA's DMUC service as opposed to DISA. Regarding the comment on identifying mobile applications approved for business use, the Samsung devices provide a means of readily identifying unmanaged applications (personal side of the device) versus managed application (business side of the device). Apple devices do not provide such a view. As a means of assisting users, the DMUC does provide listings of approved Managed and Unmanaged Apps for mobile devices; locations are noted in the General Apps FAQ located on the DMUC Mobility Portal.

Page 9 – IG Statement: *We analyzed the mobile applications downloaded by DoD mobile device users from the* [redacted] *a Component that subscribed to the DMUC. Of the* [redacted] *unique applications downloaded by* [redacted] *users, approximately* [redacted] *were unauthorized unmanaged applications that were available only from public application stores*

DISA Comment(s): This number does not accurately represent the actual quantity of unapproved apps manually downloaded by [redacted] users. As noted previously, this is very misleading to suggest all [redacted] unique applications were "downloaded by [redacted] users". The system that reported the list of apps referenced in Appendix A reports all mobile applications installed on a given device. This includes apps manually installed by the user from PUMA or the Apple App Store, apps pre-installed by the MDM, apps packaged with the operating system (OS), apps pre-installed by the Original Equipment Manufacturer (OEM), and apps pre-installed by the Mobile Network Operator. The user has no control over what "system apps" or "bloatware" get pre-installed on their DMUC device.

(U) Defense Information Systems Agency (cont'd)

SUBJECT: Defense Information Systems Agency's (DISA) response to the U.S. Department of Defense Inspector General's draft report "Management Advisory on the DoD's Use of Mobile Applications (Project No. D2021-D000CU-0143.001) 3 October 2022

Specific Recommendation Comments:

IG Recommendation #3: *We recommend that the DoD Chief Information Officer (CIO) direct DoD Component Heads and the Defense Information Systems Agency Chief Information Officer to limit the distribution of unmanaged applications to those users who can demonstrate a justifiable need for the application.*

Revised and renumbered draft Recommendation 3 as Recommendation 2.e

DISA Response #3: As written, DISA cannot restrict applications on a user-by-user basis; an application approved for one person will be available for all. Also, DISA should not serve as the "jury" for a decision on whether an application supports a mission related requirement. Our recommendation for revising this recommendation is as follows: We recommend that DoD Chief Information Officer develop policy that directs DoD component heads to justify and approve the mission requirement for all managed and unmanaged applications, and that all mobility service providers, to include the Defense Information Systems Agency, limit access to only those appropriately justified applications.

IG Recommendation #5(b): *Publish a clear list of applications approved for official business and make the list easily accessible from DOD mobile devices.*

Renumbered as Recommendation 4

DISA Response: DISA partially concurs with this recommendation. DISA publishes a list of these applications today on the mobility web portal which is accessible to mobile users. To address the recommendation, DISA will review options to make the information more easily accessible to mobile device users.

IG Recommendation #5(c): *We recommend that the Defense Information Systems Agency Chief Information Officer conduct periodic reviews, at least annually, of the list of authorized unmanaged applications and remove those without a justifiable need or with known cybersecurity risks.*

Response #5C. DISA does not agree with recommendation (c) and recommends it be removed. DISA does an initial analysis of an application before placing it in the DoD application store which exceeds DoD's requirements. Commercial Mobile Device Managers (MDMs) cannot 'remove' unmanaged apps from a device which is why we utilize supplemental mobile threat protection.

IG Recommendation #5(d): *Remove or hide any unauthorized unmanaged applications from the mobile devices of users who cannot demonstrate justifiable need for the application.*

Response #5(d). DISA does not agree with recommendation (d) and recommends it be removed. Commercial Mobile Device Managers (MDMs) cannot 'remove' unmanaged apps from a device which is why we utilize supplemental mobile threat protection. Additionally, DISA cannot be held responsible for actions related to the business justification of any application.

(U) Defense Information Systems Agency (cont'd)

SUBJECT: Defense Information Systems Agency's (DISA) response to the U.S. Department of Defense Inspector General's draft report "Management Advisory on the DoD's Use of Mobile Applications (Project No. D2021-D000CU-0143.001) 3 October 2022

IG Recommendation #5(e): *Revise the New Application Request form to ask whether the Component intends to use the application to conduct official DoD business and processes requests that answer "YES" to this question as managed applications.*

Response #5(e). DISA does not agree with recommendation (e) and recommends it be removed. DISA processes are to align with policy published by the DoD CIO. In addition, DISA cannot be held responsible for reviewing/considering the business justification of any requested applications. Finally, many of the applications requested to be added to a DoD store may be used for mission support purposes in conducting official DoD business (e.g., vendor travel applications). However, such applications should not be categorized as "managed" as they potentially could be given access to DoD controlled unclassified information.

We appreciate the opportunity to review and comment on the report and recommendations. The point of contact for this audit is [redacted]

GREENWELL.ROGER.S[redacted]
COTT.SR[redacted]

ROGER S. GREENWELL
Chief Information Officer

cc:
[redacted]

(U) Chief Digital and Artificial Intelligence Office Directorate for Digital Services

~~CUI~~

Chief Digital & Artificial Intelligence Office
9010 DEFENSE PENTAGON, ROOM 3A268
WASHINGTON, D.C. 20301-1600

October 25, 2022

MEMORANDUM FOR DoD Office of the Inspector General

SUBJECT: (U) Comments on Draft Management Advisory D2021-D000CU-0143.001

(U) As requested, this memo sets out response to recommendations on the draft management advisory on behalf of the organization formerly known as the Defense Digital Service (DDS), which is now the Chief Digital and Artificial Intelligence Office' Directorate for Digital Services (CDAO/DDS).

~~(CUI)~~ DDS disagrees with the implication that DDS personnel have been authorized to use [redacted] or other approved unmanaged or unapproved applications for official business. DDS personnel have not been authorized to use such applications for official business. DDS agrees with the balance of the recommendation, and to accomplish it DDS will withdraw the referenced authorization issued by the previous Director, and communicate such to the organization which requested the authorization. Furthermore, DDS will issue a memorandum reminding DDS personnel that official business should not be conducted using [redacted] or other approved unmanaged or unapproved applications, and to forward any available records of official business to official messaging accounts. DDS has a planned completion date of October 31, 2022, to accomplish both of these actions.

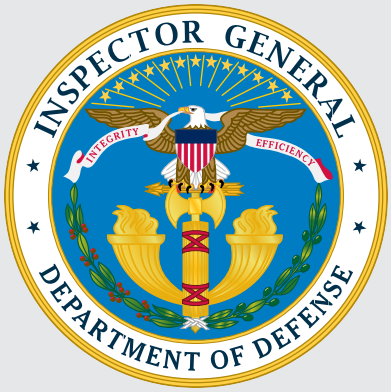
(U) Questions regarding this response should be directed to [redacted]

OLSON.KATH[redacted]
ERINE.M[redacted]

KATHERINE OLSON
Director for Digital Services
Chief Digital and Artificial Intelligence Office

~~CUI~~

~~Controlled by: CDAO - DDS~~
~~CUI Category: ISVI~~
~~POC:~~ [redacted]


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~CUI~~

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098

~~CUI~~