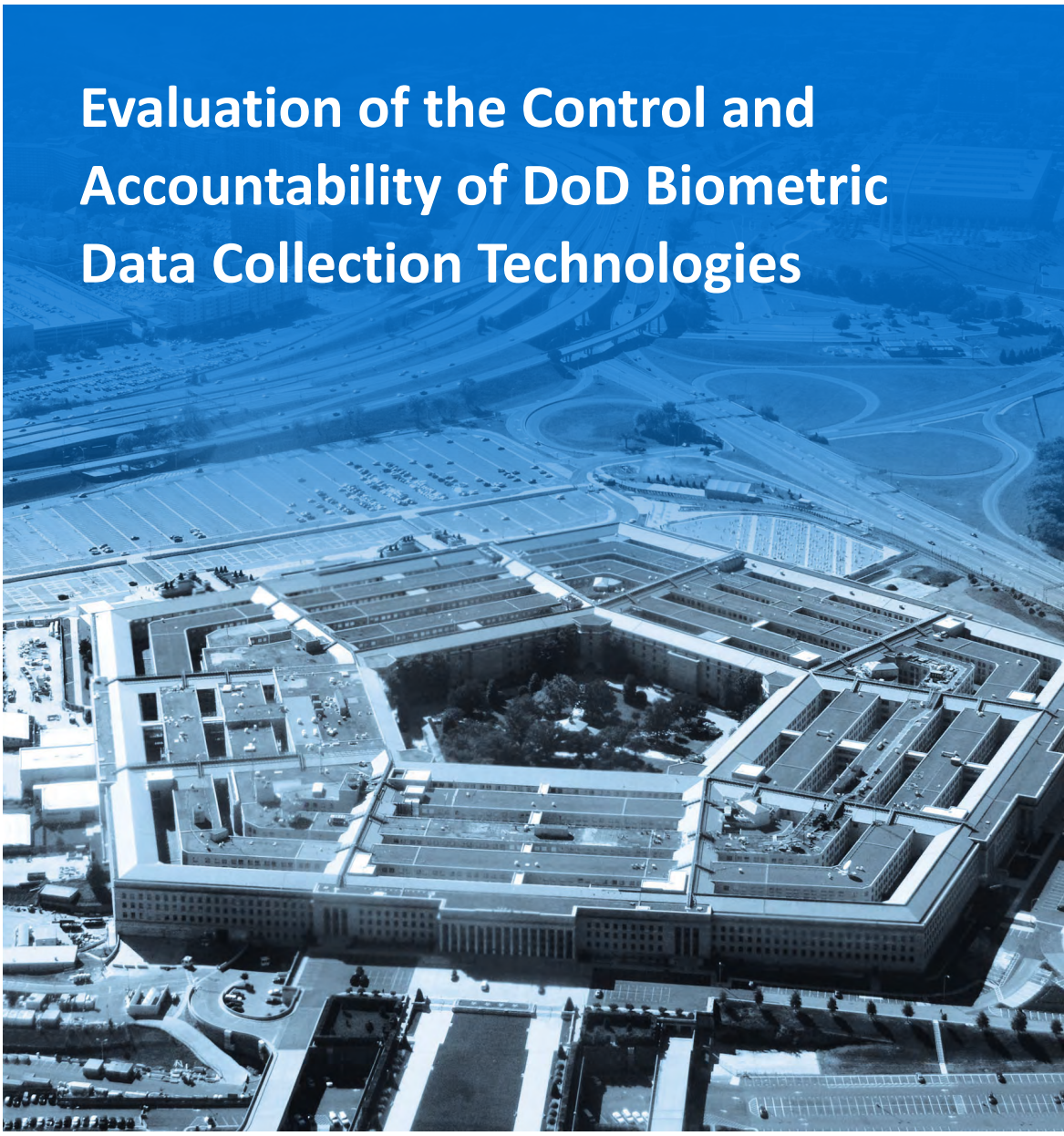
Report No. DODIG-2024-016

INSPECTOR GENERAL

U.S. Department of Defense

NOVEMBER 8, 2023

Evaluation of the Control and Accountability of DoD Biometric Data Collection Technologies



INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Evaluation of the Control and Accountability of DoD Biometric Data Collection Technologies

November 8, 2023

Objective

The objective of this evaluation was to determine whether the DoD ensured adequate control and accountability over technologies used to collect, store, and transmit biometric data to higher-level databases in overseas operations.

Background

According to DoD Directive 8521.01E, biometrics is the process of recognizing an individual based on measurable anatomical, physiological, or behavioral characteristics. The Directive defines biometric data as computer data created during a biometric process. Biometric data encompass raw sensor observations, biometric samples, models, templates, and similarity scores. Military units conducting overseas operations use biometrics to identify individuals encountered in the field, including, friendly forces, and other individuals assisting the United States, and share this information with other units and other Federal agencies. Biometric data are used to describe the information collected during an enrollment, verification, or identification process, but the term does not apply to end user information such as user name, demographic information, or authorizations.

Findings

The Services and combatant commands followed DoD policy and their own command-specific guidance and procedures to maintain property accountability for biometric devices.

However, some combatant command Service Components had biometric devices that did not have data encryption capabilities. This occurred because current DoD biometrics policy does not specify information security standards or require encryption for biometric devices.

Additionally, we found that DoD policy does not require DoD Components to provide certification of destruction or sanitization of biometric data to the Defense Logistics Agency when the devices are turned in for disposal. This occurred because there is no requirement in DoD biometric policy to confirm or verify that DoD property custodians removed biometric data from the devices before disposal.

Recommendations

We recommend that the Under Secretary of Defense for Intelligence and Security (USD(I&S)) update DoD policy to include:

- standards for encrypting and protecting data on biometric collection devices,
- a requirement to sanitize biometric data from collection devices and hard drives prior to disposal, and
- a requirement that organizations maintain records that they have sanitized all data from the biometric collection devices when the devices are turned in for disposal.

Results in Brief

Evaluation of the Control and Accountability of DoD Biometric Data Collection Technologies

Management Actions Taken

On September 27, 2023, we discussed our observations and suggested actions with the Chief of the Identity Intelligence Division from the OUSD(I&S). During our evaluation, the Chief of the Identity Intelligence Division initiated a program of actions and milestones for the development and publication of new DoD policies. Specifically, the Division Chief established a plan of actions and milestones to revise DoD policy to include standards for encrypting and protecting data on biometric devices and a requirement for custodians to sanitize data and maintain sanitization records when turning in the devices for disposal.

The Division Chief stated that they expect the revised DoD Directive to receive the necessary approvals and be published by the first quarter of FY 2025.

Our Response

These actions meet the intent of our recommendations. Therefore, we consider the recommendations resolved but open. We will close the recommendations when we receive and review the Directive that includes the modifications as stated.

Please see the Recommendations Table on the next page for the status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Under Secretary of Defense for Intelligence and Security	None	1.a., 1.b., and 1.c.	None

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – DoD OIG verified that the agreed upon corrective actions were implemented.


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

November 8, 2023

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY

SUBJECT: Evaluation of the Control and Accountability of DoD Biometric Data Collection Technologies (Report No. DODIG-2024-016)

This final report provides the results of the DoD Office of Inspector General's evaluation. We previously provided copies of the discussion draft report and held an exit conference on our finding and recommendations. We considered management actions taken when preparing the final report. We conducted this evaluation in accordance with the "Quality Standards for Inspections and Evaluations," published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency.

This report contains three recommendations that are considered resolved and open. As described in the Recommendations, Management Actions Taken, and Our Response section of this report, we will consider the recommendations closed when the Under Secretary of Defense for Intelligence and Security updates DoD Directive 8521.01E in accordance with our recommendation.

If you have any questions or would like to meet to discuss the evaluation, please contact [redacted] We appreciate the cooperation and assistance received during the evaluation.

FOR THE INSPECTOR GENERAL:

Bryan Clark

Bryan T. Clark
Acting Assistant Inspector General for
Programs and Combatant Commands

Contents

Introduction

Objective 1

Background 1

Finding. The DoD Has Adequate Accountability Controls for Biometric Collection Devices; However, the DoD Needs Improved Information Security Controls and Record Keeping 5

DoD Property Accountability Controls Are Adequate for Biometric Devices; However, the DoD Needs to Improve the Policy to Address Information Security and Disposal Records Maintenance 6

Additional Controls for the Protection of Biometric Data Would Improve Information Security 9

Recommendations and Management Actions Taken 9

Appendix A

Scope and Methodology 11

Use of Computer-Processed Data 13

Prior Coverage 13

Acronyms and Abbreviations 14

Introduction

Objective

The objective of this evaluation was to determine whether the DoD ensured adequate control and accountability over technologies used to collect, store, and transmit biometric data to higher-level databases in overseas operations.

Background

According to DoD Directive (DoDD) 8521.01E, biometrics is the process of recognizing an individual based on measurable anatomical, physiological, or behavioral characteristics.[1] The Directive defines biometric data as computer data created during a biometric process. Biometric data encompass raw sensor observations, biometric samples, models, templates, and similarity scores. Biometric data can be used to describe the information collected during an enrollment, verification, or identification process.

Military units conducting overseas operations use biometrics to identify individuals encountered in the field and share this information with other units and other Federal agencies. The DoD has used biometrics to verify common access credentials; identify personnel seeking access to installations as friend, foe, or neutral; operate detention facilities; protect DoD personnel at expeditionary bases in theater; and recover and identify U.S. personnel.

The U.S. Army, U.S. Navy, U.S. Marine Corps, and U.S. Special Operations Command (USSOCOM) provided biometric devices to personnel supporting overseas operations under the U.S. European Command, U.S. Africa Command, U.S. Central Command, USSOCOM, and their subordinate joint task forces. The DoD used a variety of handheld biometric devices, including Biometric Automated Toolsets (BAT), Secure Electronic Enrollment Kits (SEEK), the Javelin, the Biosled, as well as the Handheld Interagency Identity Detection Equipment (HIIDE), which was taken out of service in 2015.

Policies Governing Biometric Data and Devices

DoD biometrics, property accountability, and information policies govern the biometrics program and the collection, storage, and transmission of biometric data.

[1] DoD Directive 8521.05E, "DoD Biometrics," January 13, 2016 (Incorporating Change 2, October 15, 2018).

DoD Biometrics Policies and Guidance

DoDD 8521.01E establishes DoD biometrics policy and assigns responsibilities for DoD biometrics, with the Under Secretary of Defense for Research and Engineering as the office of primary responsibility. The Directive states that it is DoD policy that the maintenance, collection, use, and dissemination of biometric data, which include the transmission, storage, caching, tagging, analysis, production, and use of biometric data, adhere to applicable laws, policies, standards, and protocols. Additionally, the Directive states that biometric, biographic, behavioral, and contextual data collected and maintained by DoD Components, as well as resulting biometric-enabled intelligence products, are to be considered DoD data. The Directive further notes that such DoD data are protected from unauthorized release and shared in accordance with applicable data sharing and disclosure policy under appropriate authorities, arrangements, and agreements. The Directive designates the Under Secretary of Defense for Acquisition and Sustainment as the biometrics Principal Staff Assistant (PSA) for oversight of DoD biometric activities and policy, and the Secretary of the Army as the DoD Executive Agent for biometrics.[2]

DoD Instruction (DoDI) 3300.04 establishes DoD policy and assigns responsibilities for management and execution of biometric-enabled intelligence.[3] The Instruction states that it is DoD policy to control biometric material and data collection, transmission, storage, caching, tagging, and use through DoD-approved national, international, and other consensus-based standards, protocols, best practices, and equipment to ensure consistency and support interoperability. The Instruction directs the Under Secretary of Defense for Intelligence and Security to oversee and provide guidance on DoD biometric-enabled intelligence programs, activities, and initiatives.

DoD Property Accountability and Destruction Policies and Guidance

DoDI 5000.64 establishes policy, assigns responsibilities, and provides requirements and procedures for accounting for tangible DoD equipment and other accountable property.[4] It also outlines requirements that reflect the accountability perspective of property management, including the documentation of lifecycle events and transactions. The Instruction directs accountable property officials

[2] The policy establishes the Under Secretary of Defense for Acquisition, Technology, and Logistics as the PSA for biometrics. This position is now the Under Secretary of Defense for Acquisition and Sustainment.

[3] DoD Instruction O-3300.04, "Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI)," May 25, 2012.

[4] DoD Instruction 5000.64, "Accountability and Management of DoD Equipment," April 27, 2017 (Incorporating Change 3, Effective June 10, 2019).

to establish and maintain the organization's accountable property and financial records for government property, regardless of whether the property is in the individual's or the DoD Component's immediate control or possession. This includes the requirement for maintaining a complete trail of all transactions, suitable for audit, and the ability to implement and adhere to associated internal controls.

DoD Manual (DoDM) 4160.21, Volume 4, prescribes procedures and the sequence of processes for disposing of information technology hardware and software.[5] The Manual states that all hard drives must be overwritten, degaussed, or destroyed before "leaving" DoD control, and that the generating activities will specify which of these three disposal processes they used when transferring the property to the Defense Logistics Agency (DLA) Disposition Services sites.[6] The Manual adds that DoD Components must comply with labeling and internal documentation requirements, although when degaussing or physical destruction is the disposal process, hard drives will be transferred to DLA Disposition Services sites as scrap and do not require an affixed label. The Manual states that under the authority, direction, and control of the Under Secretary of Defense for Acquisition and Sustainment, through the Assistant Secretary of Defense (Sustainment), the DLA Director is responsible for administering the worldwide Defense Materiel Disposition Program. The Manual also directs DoD Component heads to comply with applicable Federal, state, and local laws, executive orders, and DoD policies governing materiel demilitarization and disposition.

DoD Information Governance Policies and Guidance

A July 2007 DoD Chief Information Officer memorandum established DoD policy for encryption of sensitive unclassified data at rest on mobile computing devices and removable storage media.[7] The memorandum states that it is DoD policy that all unclassified DoD data at rest that have not been approved for public release and are stored on mobile computing devices or removable storage media must be treated as sensitive data and encrypted using commercially available encryption technology. The memorandum adds that this requirement is in addition to the management and access controls for all computing devices in other DoD policies.

[5] DoD Manual 4160.21 Volume 4, "Defense Materiel Disposition: Instructions for Hazardous Property and Other Special Processing Materiel," October 22, 2015 (Incorporating Change 4, Effective December 15, 2022).

[6] Degauss is the process of destroying the data on a data storage device by removing its magnetism.

[7] DoD Chief Information Officer Memorandum, "Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media," July 3, 2007.

DoDM 5200.01, Volume 3, provides guidance for disposing of classified and unclassified information on computer media.[8] It states that all unclassified DoD data that have not been approved for public release and are stored on mobile computing devices or removable storage media must be encrypted using commercially available encryption technology.

DoDI 8500.01 establishes a DoD cybersecurity program to protect DoD information and information technology. The Instruction requires DoD Components to dispose of unclassified electronic media in accordance with the guidelines established in National Institute of Standards and Technology Special Publication 800-88.

[8] DoD Manual 5200.01 Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012 (Incorporating Change 3, Effective July 28, 2020).

Finding

The DoD Has Adequate Accountability Controls for Biometric Collection Devices; However, the DoD Needs Improved Information Security Controls and Record Keeping

DoD property accountability instructions outlined in DoDI 5000.64 provide adequate accountability controls for DoD biometric collection devices in the current inventory. In addition to DoD policy and guidance, most commands that operate biometric devices created standard operating procedures detailing more specific property accountability procedures. We reviewed hand receipts for biometric devices from across the Services and combatant commands and determined that they followed DoD property accountability policies to control biometric devices effectively.

However, the Services and combatant commands employed inconsistent information security controls on biometric devices. For example, some types of biometric devices used by U.S. Army Central and the U.S. Special Operations Command Europe do not have encryption capabilities, while other commands' devices do. This occurred because DoD biometrics policies do not provide specific instructions or requirements to secure information collected, stored, and transmitted on biometric devices. For example, DoDD 8521.01E does not specify whether biometric devices must be treated like other mobile computing devices or removable storage media in accordance with DoD information governance policy.

Additionally, Service and combatant command property custodians and the DLA did not consistently document the sanitization of biometric data at the time of disposal or retain records of those actions. This occurred because DoDD 8521.01E does not include standards for sanitizing data on biometric devices, nor does it reference existing DoD policy for documenting and recording the sanitization of data. Other factors that contribute to improper documentation and record retention include improper assignment of federal supply classification, demilitarization, and controlled inventory item codes, which aid in identifying special handling requirements.

Because the Services and combatant commands did not consistently encrypt biometric data or certify that data on biometric devices were sanitized at the time of disposal, the DoD could allow unauthorized personnel, including enemy forces, access to sensitive information.

DoD Property Accountability Controls Are Adequate for Biometric Devices; However, the DoD Needs to Improve the Policy to Address Information Security and Disposal Records Maintenance

DoD property accountability policies provide adequate controls for DoD biometric devices. However, DoD biometric devices in use at the time of this evaluation had inconsistent information security controls. In addition, property custodians and the DLA did not consistently document that DoD Components sanitized biometric devices at the time of disposal or maintain those records.

Property Accountability Controls Were Adequate For Biometric Devices

The Services and combatant commands properly followed DoDI 5000.64 and their own specific guidance and procedures to maintain property accountability for biometric devices. Because DoD guidance does not classify biometric devices as sensitive items and DoDD 8521.05E states that biometric data are unclassified, biometric devices follow standard property accountability requirements as outlined in DoDI 5000.64.

We reviewed Service and command specific policies, guidance and SOPs related to control of biometric devices to determine compliance with DoD policy. We also reviewed inventory lists, hand receipts, and other property accountability records provided by combatant commands and Service Components, such as the Navy, Army, USEUCOM, USSOCOM, and U.S. Army Europe and Africa. Specifically, for:

- the Navy, we reviewed a current inventory of 465 devices, referenced by serial number, vessel, homeport, and mission-capable status of devices.
- the Army, we reviewed a current inventory for 3,930 devices, referenced to command (FORSCOM, TRADOC, USARCENT, USASOC, etc.), unit, location, UIC, and serial number.
- USEUCOM, we reviewed a current inventory of 629 devices with sub-hand receipts to embassies, by serial number, location, and responsible officer assigned to the devices. We also reviewed sub-hand receipts for devices deployed to USAREUR-AF by serial number, Unit, UIC, and location (Hohenfels, Rhineland, Vicenza, Vilseck, and the warehouse).
- USSOCOM, we reviewed a current Inventory of 152 Biosled and 71 Seek devices, referenced to location, serial number, unit, and receipts for purchase.

We determined that the combatant commands and Service Components followed standard property accountability requirements and maintained accountability of biometric devices.

Not All Biometric Devices Used by the Services and Service Component Commands Met Data Encryption Requirements

At least two Service Components supporting overseas operations had biometric devices that did not have data encryption capabilities. According to DoDM 5200.01, Volume 3, all unclassified DoD data not approved for public release and stored on mobile computing devices or removable storage media must be encrypted using commercially available encryption technology. However, we found that at least two combatant command Service Components had biometric devices that were not encrypted. For example, personnel at both the U.S. Army Central and U.S. Special Operations Command Europe stated that their devices are not encrypted.

This occurred because current DoD biometrics policy does not specify information security standards or require encryption for biometric devices.[9] Without specific security standards in biometrics policy, DoD Components do not have consistent processes or requirements for securing their biometric information. For example, according to U.S. Army personnel, most SEEK II biometric devices have encryption technology, but neither the HIIDE devices nor the 2015 version of the SEEK II have encryption. A DoD biometrics policy standard for user authentication and encryption would provide greater consistency across the DoD and additional protection against unintended disclosure of data. Therefore, the Under Secretary of Defense for Intelligence and Security should update DoD biometric guidance to include standards for the encryption and protection of data on biometric collection devices.

The Services and Service Component Commands Did Not Consistently Certify the Destruction or Sanitization of Data When Disposing of Biometric Devices

The DoD biometric community uses different processes to sanitize the data from biometric devices and dispose of them. DoD information governance policy and guidance provide guidelines for the disposal of information and hard drives. For example, DoDM 4160.21 states that all hard drives must be overwritten, degaussed, or destroyed before leaving DoD control.

[9] The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, governs the protection of personally identifiable information ("PII"). It regulates how Executive Branch agencies and departments collect, store, use, and give out PII. The Privacy Act provides statutory privacy rights and protections only to U.S. citizens and Legal Permanent Residents. The Privacy Act does not apply to non-U.S. citizens who are not Legal Permanent Residents, also called "non-U.S. persons." (See OMB Circular A-108). However, the Judicial Redress Act of 2015 **5** U.S.C. § 552a note, extends certain rights of judicial redress established under the Privacy Act to citizens of certain foreign countries or regional economic organizations, as designated by the Attorney General. There are at least twenty-seven countries on that list, all of which have agreements with the United States regarding such protections. The biometric data discussed in this evaluation does not relate to U.S. citizens and Legal Permanent residents, nor does it relate to any citizens of the countries designated above.

U.S. Marine Corps personnel stated that they degauss all hard drives before sending devices to the DLA Disposition Services team for disposal. U.S. Special Operations Command Europe personnel noted that they send all of their devices to the USSOCOM J2 Global Security Operations Identity Intelligence Operations office for disposal. U.S. Navy personnel stated that they have not retired any devices yet, but intend to follow degaussing and collection of serial numbers of the hard drives when the time comes to retire their devices.

DoD property accountability and information governance policies require the documentation of sanitization of electronic media. DoDI 5000.64 requires maintaining a complete trail of all transactions, suitable for audit, and the ability to implement and adhere to associated internal controls. In addition, DoDI 8500.01 requires DoD Components to dispose of unclassified electronic media in accordance with the guidelines established in National Institute of Standards and Technology Special Publication 800-88. That publication states that following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. According to officials at U.S. Naval Forces Europe–Africa and U.S. Army Central, their personnel document the sanitization of data from the devices at the time of disposal on DLA Form 2500.[10]

Additionally, we found that DoD policy does not require DoD Components to provide certification of destruction or sanitization of biometric data to the DLA when the devices are turned in for disposal. Although DoD policy requires Components to fill out a standardized Issue Release/Receipt form, DLA personnel stated that DoD policy does not require those organizations to submit a DLA Form 2500 or other documentation of sanitization. We also found that the Services and combatant commands inconsistently completed the DLA Form 2500 or equivalent to confirm that biometric data were destroyed. For example, while U.S. Army Central and U.S. Naval Forces Europe–Africa used DLA Form 2500, a USSOCOM official stated that they use Form LOG-CFP-2152-A. This inconsistency occurred because, according to DLA personnel, there is no clear guidance or policy requirement for DoD property custodians to document sanitization of biometric data from the devices prior to turn-in for disposal. DLA officials added that the DLA is not authorized nor do they have the requisite expertise to verify sanitization of devices before disposal. In addition, the Services are not required to use the DLA for disposal. A policy requirement for all DoD property custodians to certify that biometric data or any other personally identifiable information are removed from devices before disposal would provide

[10] DLA Form 2500, "Certificate of Information Technology Disposition," November 2022, is used to certify that a hard drive is cleared, purged, or destroyed in accordance with DoDM 4160.21, Volume 4.

protection against unintended disclosure of biometric information collected by the DoD. Therefore, the Under Secretary of Defense for Intelligence and Security should update DoD biometric guidance to include a requirement to sanitize the data from the devices and hard drives before their disposal. The updated guidance should require organizations to maintain records of the sanitization of all data on biometric devices when those devices are turned in for disposal.

Additional Controls for the Protection of Biometric Data Would Improve Information Security

As a result of some DoD Components not encrypting biometric data and not certifying that the data are sanitized on biometric devices at the time of disposal, the DoD could allow unauthorized personnel, including adversaries, access to sensitive information. This could jeopardize force protection by providing adversaries with the biometric information and identities of friendly forces and other individuals assisting the United States. Biometric information could also provide adversaries with information to track personnel and their associates. DoD-wide standards for encryption, data protection requirements for biometric devices, and better-defined documentation requirements for biometric device sanitization would mitigate these risks.

Recommendations and Management Actions Taken

Recommendation 1

We recommend that the Under Secretary of Defense for Intelligence and Security update DoD Directive 8521.01E to:

a. Include standards for the encryption and protection of data on biometric collection devices.

b. Require the sanitization of data from devices and hard drives before disposal.

c. Require owning organizations to maintain records of the sanitization of all data on biometric devices when those devices are dispositioned for disposal.

Management Actions Taken

On September 27, 2023, we discussed our observations and suggested actions with the OUSD(I&S) Chief of the Identity Intelligence Division. During our evaluation, the Division Chief initiated a staffing action to assume the new PSA responsibilities, with an anticipated approval of its internal staffing by the end of the first quarter of FY 2024. Further, the Division Chief agreed with the other suggested actions and began implementing them. The actions include establishing standards for the encryption and protection of data on biometric collection devices, implementing

a requirement to sanitize data from devices and hard drives before disposal, and a requirement for owning organizations to maintain records of the sanitization of all data on biometric devices when those devices are dispositioned for disposal. The Division Chief developed a plan of action and milestones to revise DoDD 8521.01E to include standards for encrypting and protecting data on biometric devices and a requirement that custodians sanitize data and maintain sanitization records when turning in the devices for disposal. The Division Chief stated that they expect the revised DoDD to receive the necessary approvals and be published by the first quarter of FY 2025.

Our Response

The Division Chief's management actions taken during our evaluation meet the intent of our recommendations. Therefore, we consider the recommendations resolved but open. We will close the recommendations when we receive and review the Directive that includes the modifications as stated.

Appendix A

Scope and Methodology

We conducted this evaluation from February 2023 through August 2023 in accordance with the "Quality Standards for Inspection and Evaluation," published in December 2020 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

This evaluation focused on the Military Services and the U.S. Africa Command, U.S. Central Command, U.S. European Command, U.S. Indo-Pacific Command, and USSOCOM. In response for our requests for information, U.S. Air Force personnel stated that they did not have any biometric devices or equities in this evaluation. Additionally, U.S. Indo-Pacific Command personnel stated that their command did not have any individual collection devices.

Our evaluation focused on handheld biometric collection devices such as Biometric Automated Toolsets, Secure Electronic Enrollment Kits, Handheld Interagency Identity Detection Equipment, and Near Real Time Operations devices that collect and transmit biometric data to the DoD Automated Biometric Identification System. We excluded Defense Biometric Identification System and the Gatekeeper on the Move–Biometrics types of base access devices that tie into the Defense Manpower Data Center and Defense Enrollment Eligibility Reporting System.

We reviewed DoD, Service, and command-specific procedures, directives and instructions on the control and accountability of biometric data collection technologies, such as:

- DoD Directive 8521.01E, "DoD Biometrics;"
- DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property;"
- Army Regulation 710–2, "Supply Policy Below the National Level;"
- Secretary of the Navy Instruction 5200.42, "Accountability and Management of Department of the Navy Property;"
- U.S. Special Operations Command Regulation 700-1, "Equipment Management;"

- U.S. Central Command Regulation 525-44, "Military Operations Biometrics;"
- U.S. Army Europe Africa G34 IDEX Branch Standard Operating Procedures For Biometric Operations; and
- Combined Joint Task Force Horn of Africa Biometrics Standard Operating Procedures.

We spoke with officials from the U.S. Army Program Management Office for DoD Biometrics, select combatant commands and their Service Components or subordinate commands, and any other organizations that provide for control and accountability of biometric data collection technologies. We also examined DLA processes and procedures for safekeeping and destroying excess biometric data collection devices.

We obtained information from DoD organizations and Components, including the Secretary of the Army as the Executive Agent for Defense Biometrics; the DLA, as the responsible party for disposing of DoD excess/surplus property, including biometric data collection devices; the U.S. European Command, U.S Africa Command, U.S. Central Command, and USSOCOM; and other relevant stakeholders to determine the extent to which these laws and DoD requirements are being adequately followed.

We held meetings with officials with the Program Manager, DoD Biometrics; the Office of the Under Secretary of Defense for Intelligence and Security as the PSA responsible for oversight of DoD biometric activities and policy; the DLA; the U.S. European Command, U.S Africa Command, U.S. Central Command, U.S. Indo-Pacific Command, and USSOCOM; and Service Components and subordinate organizations to:

- determine their roles and responsibilities;
- obtain the policies and guidance they follow in their activities, including such Biometric Automated Toolsets, Secure Electronic Enrollment Kits, and Handheld Interagency Identity Detection Equipment device safekeeping and destruction requirements; and
- review their processes and procedures to determine the extent to which requirements for control, accountability, and disposition of biometric data collection technologies were followed.

We requested current inventories of biometric data collection devices and their locations to assess accountability controls for biometric devices. We also met with personnel from DLA Disposition Services to review the disposal requirements for these devices.

Use of Computer-Processed Data

We did not use computer-processed data to perform this evaluation.

Prior Coverage

During the last 5 years, the DoD Office of Inspector General (DoD OIG) issued two reports discussing biometric technologies.

Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

DoD OIG

DODIG-2022-065, "Evaluation of the Screening of Displaced Persons from Afghanistan," February 17, 2022

> This evaluation determined that the DoD had a supporting role during the biometric enrollment of Afghan evacuees in staging locations outside the continental United States and assisted in screening Special Immigrant Visa applicants. However, the DoD did not have a role in enrolling, screening, or overseeing the departure of Afghan parolees at temporary housing facilities (safe havens) within the continental United States. The evaluation found that Afghan evacuees were not vetted by the National Counter Terrorism Center using all DoD data before arriving in the continental United States. The evaluation also found that, during their analytic review, National Ground Intelligence Center personnel identified Afghans with derogatory information in the DoD Automated Biometric Identification System database who were believed to be in the United States.

DODIG-2020-062, "(U) Evaluation of Force Protection Screening, Vetting, and Biometric Operations in Afghanistan," February 13, 2020.

> (U) The objective of this evaluation was to determine whether U.S. Forces-Afghanistan (USFOR-A) developed and implemented screening, vetting, and biometric processes for force protection in Afghanistan.

Acronyms and Abbreviations

BAT	Biometric Automated Toolsets
DLA	Defense Logistics Agency
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DoDM	Department of Defense Manual
HIIDE	Handheld Interagency Identity Detection Equipment
OIG	Office of Inspector General
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PSA	Principal Staff Assistant
SEEK	Secure Electronic Enrollment Kits
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USSOCOM	U.S. Special Operations Command

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/Whistleblower-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

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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