United States Government Accountability Office

Report to Congressional Committees

August 2019

DOD INSTALLATIONS

Monitoring Use of Physical Access Control Systems Could Reduce Risks to Personnel and Assets

Accessible Version

GAO-19-649

GAO Highlights

Highlights of GAO-19-649, a report to congressional committees

August 2019

DOD INSTALLATIONS

Monitoring Use of Physical Access Control Systems Could Reduce Risks to Personnel and Assets

Why GAO Did This Study

In November 2009, an Army officer killed or wounded 45 people at Fort Hood, Texas; 4 years later in September 2013, a Navy contractor killed or wounded 16 people at the Washington Navy Yard in Washington, D.C. Independent reviews conducted in the aftermath of these shootings identified physical access control weaknesses at DOD installations.

The conference report accompanying the National Defense Authorization Act for Fiscal Year 2018 contained a provision for GAO to assess DOD's installation access control efforts. GAO (1) described actions DOD has taken to develop guidance on physical access to domestic installations and to field PACS at these installations, (2) evaluated the extent to which DOD has monitored the use of fielded PACS at these installations, and (3) evaluated the extent to which DOD has implemented an approach for addressing PACS technical issues and assessing associated performance. GAO analyzed DOD guidance on physical access control requirements, and visited installations to discuss with installation command and security force officials their experiences using PACS. This is a public version of a sensitive report that GAO issued in May 2019. Information that DOD deemed sensitive has been omitted.

What GAO Recommends

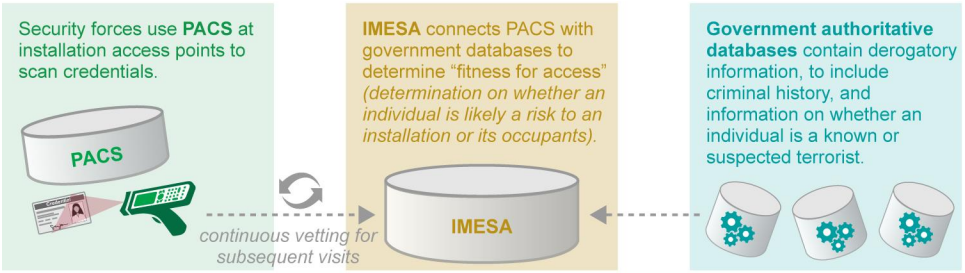
GAO made five recommendations, including that DOD monitor installations' use of PACS and develop appropriate performance measures and goals for resolving technical issues to improve PACS performance. DOD concurred with GAO's recommendations.

View GAO-19-649. For more information, contact Diana Maurer at (202) 512-9627 or maurerd@gao.gov.

What GAO Found

The Department of Defense (DOD) has issued guidance on accessing its domestic installations and strengthening physical access control systems (PACS)—used to scan credentials to authenticate the identity and authorize individuals to access DOD installations. Specifically, DOD has recently issued guidance directing the fielding of PACS and has fielded or plans to field such systems at domestic installations. The Defense Manpower Data Center (DMDC) developed the PACS used by the Air Force, the Navy, the Marine Corps, and the Defense Logistics Agency. The Army developed its own PACS. Both types of PACS electronically connect to DOD's Identity Matching Engine for Security and Analysis (IMESA). IMESA accesses authoritative government databases to determine an individual's fitness for access (i.e., whether an individual is likely a risk to an installation or its occupants), and continually vets this fitness for subsequent visits (see fig.).

PACS Connect to IMESA to Validate the Identity of Individuals and Continuously Vet Their Fitness for Access to Department of Defense Installations



IMESA Identity Matching Engine for Security and Analysis
PACS physical access control systems

Source: GAO analysis of Department of Defense information. | GAO-19-649

The Air Force and DLA have monitored their installations' use of PACS, but the Army, the Navy, and the Marine Corps have not. Army, Navy, and Marine Corps installation officials stated that they do not monitor PACS use at their installations because there is no requirement to do so. Because the Army, the Navy, and the Marine Corps do not monitor PACS use and DOD does not require that they do so, those military services do not have the data they need to evaluate the effectiveness of PACS and make informed risk-based decisions to safeguard personnel and mission-critical, high-value installation assets. DOD, Army, Navy, and Marine Corps officials agreed that monitoring installations' use of PACS would be beneficial and could be readily accomplished without significant cost using existing technology.

The Army and DMDC have used a tiered approach and established helpdesks to address PACS technical issues. The Army has established performance measures and goals to assess its approach, which has improved the ability to resolve technical issues. DMDC, however, does not have performance measures and goals, and thus lacks the information needed to evaluate its PACS' performance and address issues negatively affecting operational availability.

Contents

Tables

Figures

Abbreviations

AIE	Automated Installation Entry
DMDC	Defense Manpower Data Center
DBIDS	Defense Biometric Identification System
DOD	Department of Defense
DLA	Defense Logistics Agency
IMESA	Identity Matching Engine for Security and Analysis
PACS	physical access control systems
OUSD(I)	Office of the Under Secretary of Defense for Intelligence

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

August 22, 2019

Congressional Committees

In November 2009, an Army officer killed or wounded 45 people at Fort Hood, Texas; 4 years later in September 2013, a Navy contractor killed or wounded 16 people at the Washington Navy Yard in Washington, D.C. Independent reviews conducted in the aftermath of the Fort Hood and Washington Navy Yard shootings identified weaknesses in physical access controls at Department of Defense (DOD) installations.[1] DOD subsequently has taken action to strengthen physical access controls to protect personnel and resources on its installations.

Physical access control systems (PACS) comprise integrated hardware and software systems that security forces use at installation access control points to scan credentials (i.e., identification cards) to authenticate the identity and authorize access for individuals seeking access to DOD installations. DOD's Defense Manpower Data Center (DMDC) manages the PACS called the Defense Biometric Identification System (DBIDS) fielded at Air Force, Navy, Marine Corps and Defense Logistics Agency (DLA) installations.[2] The Army manages the PACS called Automatic Installation Entry (AIE) that are fielded at Army installations.

The conference report accompanying the National Defense Authorization Act for Fiscal Year 2018 contained a provision for us to evaluate, among other things, DOD installation access control initiatives.[3] Our objectives

[1]Secretary of Defense Independent Review of the Washington Navy Yard Shooting, *Security from Within: Independent Review of the Washington Navy Yard Shooting* (November 2013); DOD Independent Review Related to Fort Hood, *Independent Review Related to Fort Hood, Protecting the Force: Lessons Learned from Fort Hood* (January 2010). DOD Manual 5200.08 Volume 3*, Physical Security Program: Access to DOD Installations* (Jan. 2, 2019) defines an "installation" as the grounds of, but not buildings on, a base, camp, post, station, yard, center, homeport facility for any ship, or other activity under DOD jurisdiction, including any leased facility located within the United States that has a perimeter barrier (such as a fence line or wall), one or more access control points, and a method for processing visitors, except for any facility used primarily for civil works, rivers and harbors projects, or flood control projects.

[2]DMDC is a center within the Office of the Under Secretary of Defense for Personnel and Readiness that oversees the fielding and maintenance of DBIDS. We use the term "fielding" to refer to both the deployment and use of PACS.

[3]H.R. No. 115-404, at 944-45 (2017) (Conf. Rep.).

were to (1) describe actions DOD has taken to develop guidance on physical access to domestic installations and to field PACS at these installations, (2) evaluate the extent to which DOD components have monitored the use of fielded PACS at these installations, and (3) evaluate the extent to which DOD has implemented an approach for addressing PACS technical issues and assessing associated performance.

This report is a public version of a sensitive report that we issued on May 31, 2019.[4] The sensitive report included an objective related to the extent to which security forces at various DOD domestic installations used fielded PACS. DOD deemed a significant portion of the information related to this objective to be sensitive, necessitating protection from public disclosure. This public report omits information related to our observations of PACS use at these installations and the risks associated with not using PACS. As a result of this omission, we updated the wording of the second objective to focus on DOD components' efforts to monitor the use of fielded PACS at installations. Although the second objective and the information associated with it in this public report is more limited, we relied on the same methodology to support our findings and the excluded information does not impact our recommendations. The first and third objectives in this report are the same as the objectives in the sensitive report and each uses the same methodology as in the sensitive report. DOD deemed some of the detailed information presented in conjunction with the third objective to be sensitive, necessitating protection from public disclosure. As a result, this public report omits specific details regarding technical issues of PACs.

We examined physical access controls at authorized access control points at DOD domestic installations that are subject to the jurisdiction, the administration, or in the custody of the Army, the Navy, the Air Force, the Marine Corps, and DLA (which we refer to collectively as the DOD components).[5] We focused on DOD's physical access controls for

[4]GAO, *DOD Installations: Monitoring the Use of Physical Access Control Systems Could Reduce Risks to Personnel and Assets*, GAO-19-316SU (Washington, D.C.: May 31, 2019).

[5]By "domestic" installations, we are referring to active-duty DOD installations in the continental United States.

individuals seeking "unescorted access" at authorized access control points.[6]

For objective one, we reviewed and analyzed key Office of the Under Secretary of Defense for Intelligence (OUSD(I)) and DOD component policies outlining physical access control requirements and DOD component documentation, and interviewed officials from these organizations to discuss planned PACS enhancements.

For objective two, we analyzed OUSD(I), DOD component, and installation guidance on PACS use, and selected and conducted site visits to six domestic installations to meet with installation command and security force officials to discuss their experiences using PACS. In selecting the six installations, we considered one from each DOD component, geographic proximity among installations, and the type of PACS used by the installation. Of the six installations, five had fielded PACS at the time of our visit. We also reviewed OUSD(I) and DOD component policies that govern access control for standalone facilities and enclaves, but we did not evaluate the standalone facilities' and enclaves' use of PACS.[7] We then compared the guidance on the use of PACS and our observations of the five selected installations' use of PACS with *Standards for Internal Control in the Federal Government*, which states that management should obtain data on a timely basis so that they can be used for effective monitoring.[8]

For objective three, we analyzed DOD component data on the number and type of PACS' technical issues reported by DOD installations from

[6]According to DOD Manual 5200.08 Volume 3, "unescorted access" is a type of access where an individual is able to travel unaccompanied on an installation. We did not consider actions DOD has taken to prevent unauthorized access to its installations by means such as tunneling under or climbing over perimeter barriers. We recently issued a report on physical access controls used by non-DOD federal agencies to regulate visitor access to their buildings. *See* GAO, *Federal Building Security: Actions Needed to Help Achieve Vision for Secure, Interoperable Physical Access Control,* GAO-19-138 (Washington, D.C.: Dec. 20, 2018).

[7]According to OUSD(I) officials, "standalone facilities" are access-controlled structures outside of an installation, such as education and training centers, that are under the authority, direction, and control of DOD. "Enclaves" are areas within an installation, such as airfields and operations centers, that are under the authority, direction, and control of DOD and have more restrictive access controls than the installation.

[8]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: September 2014).

January 2016 through July 2018. We also compared the steps the Army and DMDC have taken or planned to address helpdesk technical issues with *Standards for Internal Control in the Federal Government* for developing performance measures.[9] We interviewed officials from DOD components and the installations we visited to discuss their experiences with PACS helpdesks, and their views on the performance and reliability of PACS. We assessed the reliability of the technical issue data by interviewing knowledgeable officials about steps taken to verify the data's accuracy, and tested the raw data to determine the accuracy of the summary data provided by DOD. We determined that the data were sufficiently reliable for our understanding of the number and types of PACS technical issues. More detailed information on our objectives, scope, and methodology can be found in appendix I of this report.

We conducted this performance audit from February 2018 to August 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We subsequently worked with DOD from June 2019 to August 2019 to prepare this public version of the original sensitive report. This public version was also prepared in accordance with these standards.

Background

It is DOD policy that installations, property, and personnel shall be protected and that the authority of a DOD commander to take reasonably necessary and lawful measures to maintain law and order and to protect installation personnel and property includes the individuals' removal from or denial of access to, an installation when those individuals threaten the orderly administration of the installation.[10] The Under Secretary of Defense for Intelligence develops overall security policy, including

[9]GAO-14-704G.

[10]DOD Instruction 5200.08, *Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)* (Dec. 10, 2005) (incorporating change 3, effective Nov. 20, 2015).

requirements for the DOD Physical Security Program, and the secretaries of the military departments and heads of DOD components establish policies and procedures to implement the Under Secretary's policies.

DOD's Process for Determining Whether to Grant Unescorted Access to Individuals Seeking Access to DOD Installations

Individuals may seek unescorted, escorted, or trusted traveler access to DOD installations.[11] As previously mentioned, this report focuses on individuals seeking unescorted access.

Unescorted installation access requires, with limited exceptions, individuals seeking access to establish their identity, be determined fit for access, and establish an acceptable purpose for their presence on the installation.[12] DOD components' security forces establish the identity of individuals at authorized installation control points by using identification credentials, specifically a DOD-issued common access card or other credentials listed in DOD guidance.[13] DOD's Identity Matching Engine for Security and Analysis (IMESA), which is maintained by the Under Secretary of Defense for Personnel and Readiness, helps security forces make current fitness-for-access determinations for installations that have

[11]According to DOD Manual 5200.08 Volume 3, if an individual is granted "escorted access," the escort—who possesses an acceptable credential and has satisfied the requirements for installation access—must remain within reasonable visual contact of those being escorted at all times. Individuals can also seek access under the trusted traveler program that allows authorized individuals who have been granted unescorted access to simultaneously vouch for individuals (in the same vehicle or on foot) and enable those individuals to obtain trusted traveler access to the installation. The trusted traveler program is intended, in part, to expedite access to installations for certain individuals and mitigate traffic congestion on adjoining highways.

[12]According to DOD Manual 5200.08 Volume 3, determining fitness for access has two elements: historic fitness and current fitness. "Historic fitness" is a determination that an individual's criminal history reflects a level of character and personal conduct that does not pose a risk to the safety, security, and efficiency of an installation or its occupants. "Current fitness" is a determination that an individual has no pending criminal cases or actions and is not on any U.S. government terrorism lists that would indicate that the individual may pose a risk to the safety, security, and efficiency of the installation or its occupants.

[13]DOD issues a unique identification credential called a common access card to military personnel, civilian employees, and eligible contractors. According to DOD Manual 5200.08 Volume 3, in addition to DOD's common access card, other credentials listed in DOD guidance include military dependent and DOD retiree identification cards.

PACS that connect to IMESA.[14] IMESA electronically links PACS to federal government (including DOD's) and local population databases to verify information contained in individuals' credentials and to search for derogatory information.[15] IMESA continuously vets individuals for fitness-for-access determinations against these authoritative government databases every 24 hours.[16] If derogatory information is found, IMESA is to send an alert to the PACS so that security forces can take appropriate action if and when those individuals next seek access to installations.

Individuals without a common access card or another acceptable credential who seek access to installations with PACS are sent through the installations' visitor control process where security forces are to (1) authenticate the individuals' identity, (2) establish an acceptable purpose for their presence on the installations, and (3) make fitness-for-access determinations using any derogatory information from authoritative government databases. These databases could include those accessible through IMESA, where available and as applicable.[17] Figure 1 illustrates

[14]According to DOD Manual 5200.08 Volume 3, for the purposes of controlling access to DOD installations, DOD has three types of installations: those that have PACS that are connected to IMESA, those that have PACS that are not connected to IMESA, and those without PACS. This report focuses on installations that have PACS that are connected to IMESA.

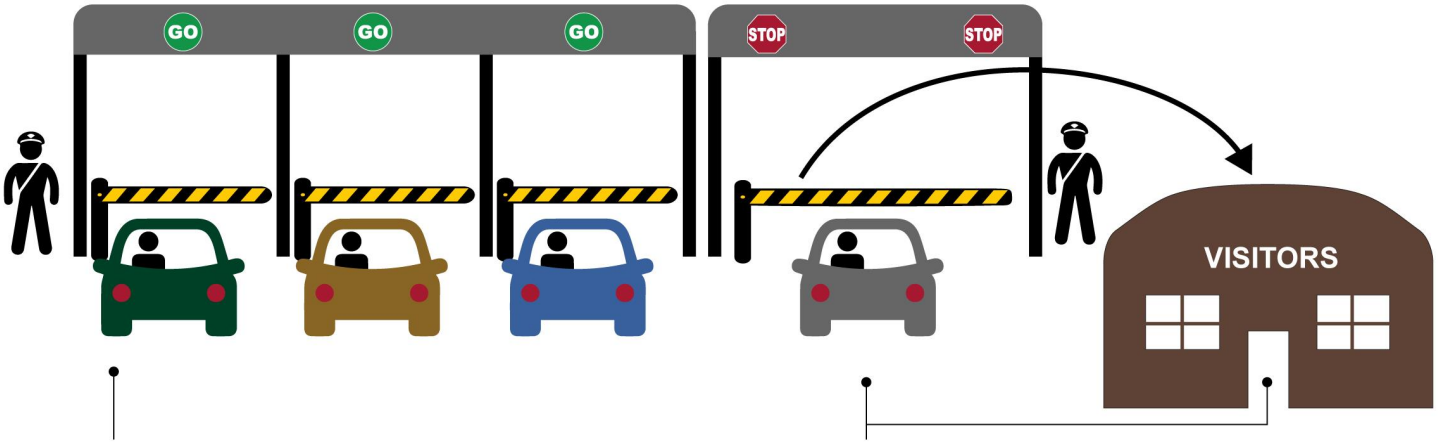
[15]Local population databases contain information on individuals with a valid reason to access the installation who are not already recorded in the Defense Enrollment Eligibility Reporting System and whose credential is authorized to facilitate access to a DOD installation. DOD installations develop and maintain local population databases to track individuals who have had their credential processed through a visitor control center or PACS at least once. According to DOD Manual 5200.08 Volume 3, derogatory information is information that reflects negatively on the integrity or character of an individual. Examples of derogatory information include, but are not limited to, aspects of an individual's criminal history.

[16]"Vetting" is an evaluation of an individual's character and conduct for approval, acceptance, or denial for the issuance of a physical access control credential. Although DOD can use the term "continuous vetting" to refer to different processes in different contexts, for the purposes of this report we refer to continuous vetting as the recurring review of an applicant's character and conduct against authoritative government databases to determine fitness for access to DOD installations. Authoritative government databases include official personnel and industrial security and law enforcement data sources.

[17]In this report, we use "acceptable credential" to refer to (1) a credential that can be automatically enrolled in IMESA and an installation's PACS, such as certain DOD-issued credentials (e.g., the common access card), or (2) another credential, such as a state-issued driver's license, that has previously been enrolled through an installation's visitor control center process including enrollment in IMESA, if available, and an installation's PACS and whose enrollment is unexpired.

the process for gaining unescorted access to installations with PACS that connect to IMESA—both for individuals with and without acceptable credentials.

Figure 1: Process for Gaining Unescorted Access to Installations with PACS That Connect to IMESA



Individuals with acceptable credentials

- Individuals with acceptable credentials check in at the installation access control point.
- The PACS eletronically connects to IMESA to vet the individuals for fitness for access.[a]
- If no derogatory information[b] is found and purpose for presence on the installation is established, if necessary, the individuals are granted unescorted access to the installation.

Individuals without acceptable credentials

- The visitor lane is the access point for individuals without an acceptable credential.
- The individuals are sent through the visitors control process.
- Security forces authenticate the individuals' identity and validate if there is an acceptable purpose for presence on the installation.[a]
- If no derogatory information[b] is found in government authoritative databases, which could include the use of IMESA, the individuals are issued either a short- or long-term visitors pass, or enrolled on the basis of the purpose for presence on the installation.

DOD	Department of Defense
IMESA	Identity Matching Engine for Security and Analysis
PACS	physical access control systems

Source: GAO analysis of DOD documents. | GAO-19-649

Note: "Unescorted access" is the type of access with which an individual is able to travel unaccompanied on an installation.

[a]"Fitness for access" is a determination based on historic and current information that an individual is likely not a risk to the safety, security, and efficiency of an installation or its occupants.

[b]"Derogatory information" is information that reflects negatively on the integrity or character of an individual. Examples of derogatory information include, but are not limited to, aspects of an individual's criminal history.

Types of PACS That DOD Components Have Fielded and IMESA's Capabilities

DOD components have fielded the following types of PACS at their domestic installations:

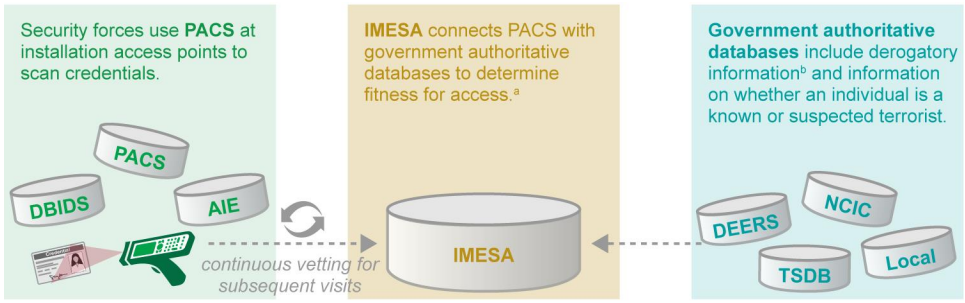
- **DBIDS.** DMDC developed DBIDS and it is used by the Air Force, the Navy, the Marine Corps, and DLA to control access to their respective installations. DBIDS consists of hardware and software—specifically, computers, servers, badge printers, and handheld identification devices. DBIDS has the capability to electronically connect to authoritative government databases using IMESA.
- **AIE.** The Army developed AIE to control access to its installations. AIE consists of hardware and software—specifically, computers, servers, badge printers, and handheld identification devices. AIE also includes additional hardware such as gate arms and automated pedestals where individuals can scan their own credentials. AIE has the capability to electronically connect to authoritative government databases using IMESA.
- **RAPIDGate.** RAPIDGate is a legacy system that according to DMDC officials is no longer being fielded to DOD installations and, according to Army officials, as of October 2018 was in use at only four domestic Army installations.[18] RAPIDGate does not have the capability to electronically connect to authoritative government databases.

Deployed by DOD in 2014, IMESA verifies enrolled individuals' information against (1) DOD's Defense Enrollment Eligibility Reporting System to determine if the credentials have been revoked; (2) the Federal Bureau of Investigation's National Crime Information Center's Wanted Persons file to determine if there are records on the individuals for an outstanding felony warrant; (3) the Federal Bureau of Investigation's Terrorist Screening Database to determine if the individuals are known or suspected terrorists; and (4) the local population database, according to an OUSD(I) official, to determine if credentials issued by installations

[18]According to Army officials, the Army plans to replace RAPIDGate with AIE at these four installations by fiscal year 2021. The Navy and the Marine Corps transitioned from RAPIDGate to DBIDS in 2017 and 2018, respectively, according to Navy and Marine Corps officials.

have been revoked or have expired.[19] Individuals with enrollable credentials are enrolled in IMESA when their credentials are scanned by PACS for the first time. According to DMDC officials, once individuals are enrolled, IMESA continuously vets them against these authoritative government databases every 24 hours and it takes approximately 2 seconds for each individual's credential to be vetted through IMESA. Figure 2 illustrates the process of using PACS to electronically connect to IMESA to validate individuals' identity and continuously vet individuals' fitness for access to DOD installations.

Figure 2: PACS Connect to IMESA to Validate the Identity of Individuals and Continuously Vet Their Fitness for Access to Department of Defense Installations



AIE	Automated Installation Entry	NCIC	National Crime Information Center
DBIDS	Defense Biometric Identification System	PACS	physical access control systems
DEERS	Defense Enrollment Eligibility Reporting System	TSDB	Terrorist Screening Database
IMESA	Identity Matching Engine for Security and Analysis		

Source: GAO analysis of Department of Defense documents. | GAO-19-649

[a]"Fitness for access" is a determination based on historic and current information that an individual is likely not a risk to the safety, security, and efficiency of an installation or its occupants.

[b]"Derogatory information" is information that reflects negatively on the integrity or character of an individual. Examples of derogatory information include, but are not limited to, aspects of an individual's criminal history.

[19]DOD's Defense Enrollment Eligibility Reporting System contains identifying information—such as social security numbers and benefits eligibility status—for uniformed service members, U.S.-sponsored foreign military service members, DOD and uniformed services civilians, and other personnel as directed by DOD. The National Crime Information Center is an electronic clearinghouse of local, state, and federal criminal history data administered by the Federal Bureau of Investigation. The center's Wanted Persons File includes records on individuals for whom a federal warrant or a felony or misdemeanor warrant is outstanding. According to OUSD(I) officials, the source for all of the IMESA warrant alerts is the felony-level Wanted Persons File. The Terrorist Screening Database is the government's authoritative consolidated database that contains information on individuals who are known or reasonably suspected to have been involved in preparing for, aiding, or engaged in conduct relating to terrorist activities.

Roles and Responsibilities Related to Physical Access Controls

The Under Secretary of Defense for Intelligence is responsible for establishing department-wide physical access control standards, procedures, and guidance, consistent with DOD guidance and applicable laws, to include developing processes for establishing the identity of individuals seeking access to installations. The Under Secretary of Defense for Personnel and Readiness is responsible for designing and maintaining IMESA, and establishing and executing a plan to integrate IMESA with PACS at all DOD installations. DMDC is a center within the Office of the Under Secretary of Defense for Personnel and Readiness that provides identity management services and oversees the fielding and maintenance of DBIDS. DOD components issue their own component- and installation-specific requirements for physical access control. These include physical access barrier requirements such as fences, as well as the use of PACS.

Each DOD component has designated a program manager to supervise and oversee its physical security program, to include PACS. According to DOD component guidance and officials:

- The Army Acquisition Corps, Product Manager for Force Protection Systems, is responsible for the procurement and fielding for the Army's PACS. The Army Office of the Provost Marshal General develops PACS requirements based on DOD and Army policies for the Army's physical security program.
- The Commander Navy Installations Command is responsible for the Navy's PACS.
- The Air Force Security Forces Center is responsible for the Air Force's PACS. The Office of the Deputy Chief of Staff for Logistics, Engineering, and Force Protection, Directorate of Security Forces, is responsible for developing service-wide access control policies.
- The Commander, Marine Corps Installations Command, is responsible for the Marine Corps' PACS. The Deputy Commandant, Plans, Policies, and Operations establishes policies, sets requirements, and is responsible for the Marine Corps' Physical Security Program.
- DLA Information Operations and Installation Support Security and Emergency Services Staff Directors share responsibility for the DLA's PACS.

Additionally, DOD component installation commanders are responsible for the physical security of their installations, including for the use of PACS.

DOD Has Issued Guidance on Physical Security, Fielded or Planned to Field PACS, and Identified Future Enhancements

DOD Has Recently Issued Department-wide Guidance for Controlling Installation Physical Access, and Fielded or Planned to Field PACS at All Domestic Installations

OUSD(I) issued a physical security manual in January 2019 that addresses minimum department-wide standards for access to DOD installations.[20] The manual incorporates and cancels Directive-Type Memorandum 09-012, the interim policy for DOD physical access control that was in effect for about 9 years.[21] The manual directs DOD components to, among other things, implement procedures for all populations to gain access to component installations; field electronic PACS at all DOD installations; and fund the continued operation, maintenance, and enhancement of IMESA with additional government data sources. The manual also states that new electronic PACS and existing electronic PACS undergoing significant upgrades (valued at more than 50 percent of replacement cost) must interface with IMESA.

Each DOD component had also issued guidance on installation physical access control standards that pre-date the January 2019 physical security

[20]DOD Manual 5200.08 Volume 3, *Physical Security Program: Access to DOD Installations* (Jan. 2, 2019).

[21]DOD *Directive-Type Memorandum 09-012, Interim Policy Guidance for DOD Physical Access Control* (Dec. 8, 2009) (incorporating change 9 effective Aug. 23, 2018) (incorporated and cancelled by DOD Manual 5200.08 Volume 3 on January 2, 2019). According to an OUSD(I) official, the interim policy was used while OUSD(I), DOD components, and other DOD stakeholders developed consistent definitions and standards for physical access controls for DOD installations.

manual.[22] For example, DLA Manual 5200.08 Volume 1 identifies DBIDS as DLA's PACS and requires certain installation commanders to incorporate and maximize the use of electronic credential authentication. In another example, Army Regulation 190-13 assigns installation commanders responsibility for implementing AIE, when available, and states that deviations from the Army AIE standards and specifications are not authorized without written approval from Army headquarters. DOD component officials said that they will update their guidance to incorporate the DOD installation access control standards contained in OUSD(I)'s 2019 physical security manual.

To implement these department-wide access control standards, according to OUSD(I) and DOD component officials, each DOD component has fielded or plans to field PACS that connect to IMESA at all their domestic installations.[23] According to DOD component officials, as of February 2019, the Air Force, the Navy, the Marine Corps, and DLA have fielded DBIDS at all of their domestic installations. Specifically, according to DOD component officials, DBIDS is fielded at:

- 67 Air Force installations
- 56 Navy installations
- 16 Marine Corps installations
- 5 DLA installations

According to Army officials, as of February 2019, AIE was fielded at 35 of the Army's domestic installations. The officials stated that the Army

[22]Army Regulation 190-13, *The Army Physical Security Program* (Feb. 25, 2011) (effective Mar. 27, 2011); Air Force Manual 31-113, *Installation Perimeter Access Control* (Feb. 2, 2015) (incorporating changes from Air Force Guidance Memorandum 2018-01, effective Apr. 4, 2018); Commander Navy Installations Command Instruction 5530.14A, *Commander Navy Installations Command Ashore Protection Program* (June 6, 2016) (change transmittal 2); Marine Corps Order 5530.14A, *Marine Corps Physical Security Program Manual* (June 5, 2009); Marine Corps Installation Command Policy, *MCICOM Installation Physical Access Control Policy* (September 2015); DLA Instruction 5200.08 Volume 1, *Physical Security Program* (July 21, 2017); and DLA Manual 5200.08-V1, *Physical Security* (July 15, 2016).

[23]In an August 2018 memorandum, the Under Secretary of Defense for Intelligence directed the secretaries of the military departments to develop plans, if none are already complete, to field and use IMESA-integrated PACS at all domestic installations by September 30, 2019. Under Secretary of Defense for Intelligence Memorandum, *Plan for the Deployment of Identity Matching Engine for Security and Analysis and Vetting of Individuals* (Aug. 27, 2018).

currently plans to field AIE at an additional 60 installations by September 2019, and at all of its remaining domestic installations by the end of fiscal year 2021. However, Army officials told us that, at the direction of the Secretary of the Army, AIE is undergoing additional testing and assessment to inform a comparison with DBIDS. The Secretary of the Army is expected to make a decision sometime in summer 2019 on which PACS to field at remaining Army installations.

DMDC Has Identified Future Enhancements to IMESA and DBIDS, and the Army Has Identified Future Enhancements to AIE

DMDC plans to enhance IMESA's capabilities to allow for increased information sharing and vetting, and to expand the type of credentials that DBIDS can scan. Specifically, the Under Secretary of Defense for Intelligence has identified additional authoritative government databases that IMESA will connect with to access derogatory information.[24] For example, the Under Secretary of Defense for Intelligence directed the secretaries of the military departments to develop a plan to vet individuals seeking unescorted access to domestic installations for disqualifying derogatory information in additional files within the National Crime Information Center's database and the Interstate Identification Index by September 30, 2019.[25] According to an OUSD(I) official, IMESA will be able to access two additional National Crime Information Center files by 2020: the National Sexual Offender Registry File and the Violent Persons File. The official also stated that there are plans to connect IMESA to DOD's Automated Biometric Identification System by 2020.[26]

[24]Under Secretary of Defense for Intelligence Memorandum, *Plan for the Deployment of Identity Matching Engine for Security and Analysis and Vetting of Individuals* (Aug. 27, 2018).

[25]As previously mentioned, the National Crime Information Center's database comprises various law enforcement files. Currently, IMESA connects to only one of those files, the Wanted Persons file, which contains records on individuals for whom a federal warrant or a felony or misdemeanor warrant is outstanding. The Interstate Identification Index is a federal and state system used to exchange criminal history records.

[26]The Automated Biometric Identification System is DOD's system for matching, storing, and sharing biometric data in support of military operations with other government agencies and with partner nations. The system is used by DOD to identify and verify non-U.S. citizens to help determine if the individuals pose an immediate or potential threat to national security.

DMDC plans to expand the types of credentials that DBIDS can scan, to include all credentials listed in DOD's 2019 physical security manual.[27] For example, according to DMDC officials, scheduled enhancements to DBIDS will enable security forces to scan cards and driver's licenses compliant with the REAL ID Act of 2005 by the end of fiscal year 2019.[28] Moreover, according to DMDC officials, this enhancement will eliminate the time and expense to annually issue and print hundreds of thousands of temporary DBIDS credentials. The officials also stated that DMDC has plans to enable DBIDS handheld devices to read military veterans' health identification cards, although no time frame for implementation has been set.

Army Office of the Provost Marshal General officials told us that AIE can already scan identification cards and driver's licenses compliant with the REAL ID Act. This capability allows individuals with these credentials to be vetted and enrolled in IMESA in the access control lane without having to go the visitor control center. According to Army officials, this "in-lane" initial vetting and IMESA enrollment takes approximately 30 seconds by checking the National Crime Information Center database and Interstate Identification Index for criminal history and active warrants. Further, these officials told us that the Army has also identified future enhancements to AIE, such as transitioning to a cloud-based version. The officials told us that a cloud-based version of AIE will allow for quicker and more cost-effective fielding because of fewer installation prerequisites and reduced computer hardware requirements. Army officials are also considering other enhancements, such as self-service kiosks and web-based registration options, to streamline and expedite initial visit registrations.

[27]According to an OUSD(I), official, there are a small number of installations that, with approval from DOD component leadership, accept credentials not listed in DOD guidance.

[28]The REAL ID Act of 2005, Pub. L. No. 109-13, §§ 201-207 (2005) (codified, as amended, at 49 U.S.C. § 30301 note) establishes minimum security standards for license issuance and production, and prohibits federal agencies, including DOD installations, from accepting driver's licenses and identification cards for certain purposes from states not meeting the act's minimum standards. The Department of Homeland Security presently enforces the REAL ID Act in accordance with a phased enforcement schedule and regulatory time frames. The REAL ID Act requires these identification cards and driver's licenses to include certain information and a common machine-readable technology.

The Air Force and DLA Have Monitored the Use of PACS, but the Army, the Navy, and the Marine Corps Have Not

The Air Force and DLA monitor their installations' use of PACS and the Army, the Navy, and the Marine Corps do not. As a part of our work, we conducted numerous site visits to domestic installations to observe the DOD components' use of PACS, but details concerning our findings associated with these visits are omitted because the information was deemed sensitive by DOD. Air Force and DLA officials stated they routinely collect data on PACS use and the number of credentials scanned at their installations and provide those data to their leadership. Additionally, the Air Force is using these data to brief installation commanders on the risks associated with not using DBIDS at their installations. Army, Navy and Marine Corps officials stated they do not monitor PACS use at their installations because there is not a requirement to do so. Our review of DOD guidance also found no such requirement.

DOD component officials emphasized the importance of installation commanders having discretion to make risk-based decisions regarding access control in general, and in deciding when or when not to use PACS. Nevertheless, OUSD(I), Army, Navy, and Marine Corps officials agreed that monitoring installations' use of PACS would be beneficial and could be readily accomplished without significant cost using existing technology. For example, Army, Navy, and Marine Corps officials stated that their installations could collect monthly scanning data using existing PACS reporting mechanisms to identify below average use and determine if actions are needed to increase use. One OUSD(I) official further stated that, depending on the extent to which installations are not using PACS, changes to guidance might be warranted to require monitoring of the use of PACS.

DOD Instruction 5010.40, *Managers' Internal Control Program Procedures* directs the Office of the Secretary of Defense and DOD component heads to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to periodically evaluate the effectiveness of those

controls.[29] Furthermore, *Standards for Internal Control in the Federal Government* for performing monitoring activities states that management should monitor and evaluate the results of its internal control systems by obtaining relevant data on a timely basis, and determine appropriate control actions for any identified deficiencies.[30]

Because the Army, the Navy, and the Marine Corps do not monitor the use of PACS and because OUSD(I) does not require that they do so, those military services do not know the extent to which PACS are being used at more than 100 installations. Consequently, the military services do not have the data they need to evaluate the effectiveness of PACS and inform risk-based decisions to safeguard personnel and mission–critical, high-value installation assets.

Demonstrating the importance of using PACS that connect to IMESA, we note that, according to DMDC, IMESA has identified more than 42,000 instances of individuals who were granted access to a DOD installation and were subsequently issued a felony warrant.[31]

[29]DOD Instruction 5010.40, *Managers' Internal Control Program Procedures* (May 30, 2013).

[30]GAO-14-704G.

[31]According to DOD officials, the 42,000 instances represent individuals identified in the felony-level National Crime Information Center's Wanted Persons File. Additionally, because individuals can seek repeated access to installations, the 42,000 instances do not represent the number of individuals seeking access to domestic DOD installations nor do they necessarily represent crimes committed on an installation.

DMDC and the Army Have Approaches for Resolving PACS Technical Issues, but DMDC Has Not Assessed the Performance of Its Approach While the Army Has

DMDC and the Army Have Approaches and Helpdesks for Resolving PACS Technical Issues

Installation security forces call the DMDC helpdesk for assistance in resolving DBIDS technical issues. According to DMDC officials, this helpdesk handles technical issues for more than 100 DMDC applications and programs, including DBIDS, and is staffed 24 hours a day, 7 days a week. DMDC helpdesk staff classify DBIDS technical issues into one of three tiers, based on complexity and the estimated time to resolve an issue. According to DMDC officials, tier I issues tend to be the least complex and typically take the least time to resolve, whereas tier III issues tend to be the most complex and typically take the longest time to resolve. Tier II issues fall between tier I and tier III issues with respect to complexity and anticipated resolution time. Below are examples of issues that are experienced in each tier:

- Tier I. Unresponsive computer screens, passwords that need to be reset, and relatively simple network printer issues.
- Tier II. Handheld device battery charging issues, network synchronization issues, and problems installing fingerprint readers.
- Tier III. Handheld devices not connecting to servers, locked user accounts, and equipment that needs to be replaced.

According to DMDC officials, all calls to the helpdesk are initially handled by a tier I customer service representative. The tier I representative triages the issue using DBIDS reference materials, and if he or she is unable to resolve the issue it is passed to a tier II customer service representative. If the tier II representative is unable to resolve the issue using DBIDS reference materials, then, with a supervisor’s review and approval, the call is transferred to the tier III group. The issue is then assigned to either the tier III hardware group or the tier III software/application group, depending on the nature of the technical issue. According to DMDC officials, the tier III hardware group is located

in Ashburn, Virginia, and the tier III software/application group is located at DMDC's offices in Seaside, California.

The Army also has instituted a tiered approach for resolving AIE technical issues through its helpdesk. The AIE helpdesk is also staffed 24 hours a day, 7 days a week. Similar to DBIDS, the Army classifies AIE technical issues into one of three tiers, based on complexity and time to resolve. According to Army officials, all Army installation security forces' calls to the helpdesk are initially handled by a tier I customer service representative who tries to resolve the issue using AIE reference materials. If the tier I representative is unable to resolve the issue, the issue is passed to a tier II field service representative.[32] The field service representative is expected to contact the installation within 24 hours and attempt to resolve the issue by email or phone. If the field service representative is unable to resolve the issue remotely, the representative will make an in-person service visit to attempt to resolve the issue. If the issue cannot be resolved, then the customer service representative classifies the issue as tier III and transfers the issue to AIE system engineers for resolution. According to Army officials, tier III issues are usually Army-wide issues, such as problems associated with software updates.

DMDC Has Not Assessed the Performance of Its DBIDS Helpdesk but the Army Has Developed Performance Measures and Goals to Assess AIE's Performance

DMDC has collected data on DBIDS technical issues; however, DMDC has not been able to assess its performance due to a lack of performance measures and associated goals. Table 1 shows the number of DBIDS technical issues and the average time it took to resolve them, by tier, from January 2016 through July 2018. Specific details regarding the number of issues and the resolution time were omitted because the information was deemed sensitive by DOD.

[32]AIE field service representatives provide technical support to an assigned geographic cluster of installations, to include onsite repair services and equipment replacement.

Table 1: Number of Defense Biometric Identification System (DBIDS) Technical Issues and Average Resolution Time, January 2016 through July 2018

DBIDS technical issues	Tier	2016 (calendar year)	2017 (calendar year)	January-July 2018 (calendar year)
Number	I	1,542	2,706	2,057
Number	II	2,779	4,617	2,362
Number	III	5,409	6,183	4,115
Average resolution time	I	10 hours	3 hours	4 hours
Average resolution time	II	2 days 23 hours	3 days 7 hours	3 days 3 hours
Average resolution time	III	7 days 3 hours	13 days 14 hours	14 days 6 hours

Source: Defense Manpower Data Center. | GAO-19-649

Note: Tier I issues tend to be the least complex and typically take the least time to resolve, whereas tier III issues tend to be the most complex and typically take the longest time to resolve. Tier II issues fall between tier I and tier III issues with respect to complexity and anticipated resolution time.

The Army collects data on AIE technical issues and has developed performance measures and associated goals to assess AIE performance. Specifically, the AIE Reliability Analytics Model tracks real-time information on operational availability with a goal of 100 percent, the number and age of open helpdesk tickets with a goal of resolving tier II issues within 48 hours, and field service representative performance with a goal of a 100 percent closure rate for tier II issues. According to Army officials, the Army is currently developing specific targets for its tier I and tier III technical issues.

The Army has used data on AIE technical issues to improve AIE performance. For example, due to the age and number of tickets, the Army analyzed 646 AIE helpdesk tickets generated from October 2017 through February 2018 and determined that the root causes of the most prevalent technical issues were site server and handheld device failures. As a result of its analysis, the Army implemented an AIE software update and has begun fielding a more reliable brand of handheld device to installation security forces. According to Army officials, AIE operational availability has increased and technical issues are resolved more quickly since the AIE Reliability Analytics Model came online in September 2017. For example, from September 2017 through August 2018, AIE's operational availability increased from 93 percent to 98 percent and the average ticket age for all tiers decreased by 33 percent. Increased AIE operational availability allows for increased continuous vetting of

individuals seeking access to Army installations. Army officials at all levels have access to the model, and the Army Product Manager for Force Protection Systems sends weekly emails to Army leadership highlighting AIE performance achievements and challenges.

We have previously reported, that by tracking performance and developing performance measures, agencies can better evaluate whether they are making progress and achieving their goals.[33] Further, to fully address challenges agencies must be able to demonstrate progress achieved through corrective actions, which is possible through the reporting of performance measures.[34] Characteristics of effective performance measures include having baseline or trend data, setting measurable program goals, and establishing time frames for achieving goals. Program goals communicate what results the agency seeks and allow agencies to assess or demonstrate the degree to which those desired results are achieved. Both performance measures and goals give managers crucial information to identify gaps in program performance and plan any needed improvements.

Although user agreements between DMDC and the DOD components state that DMDC will provide helpdesk and maintenance support, the agreements do not include performance measures and associated goals regarding DBIDS' operational availability and the timely resolution of technical issues. DMDC officials acknowledged that performance measures and associated goals would likely reduce the time it takes to resolve DBIDS technical issues, particularly for tier II and tier III issues. However, until DMDC develops performance measures and goals, its ability to systematically address the underlying issues negatively affecting DBIDS' operational availability is hindered.

[33]For example, see GAO, *Defense Logistics: Improved Performance Measures and Information Needed for Assessing Asset Viability Initiatives*, GAO-17-183 (Washington, D.C.: Mar. 16, 2017) and *Defense Health Care Reform: Additional Implementation Details Would Increase Transparency of DOD's Plans and Enhance Accountability*, GAO-14-49 (Washington, D.C.: Nov. 6, 2013).

[34]For example, see GAO, *Determining Performance and Accountability Challenges and High Risks,* GAO-01-159SP (Washington, D.C.: Nov. 1, 2000) and GAO, *High Risk Series: An Update*, GAO-11-278 (Washington, D.C.: Feb. 16, 2011).

Conclusions

Although according to DOD officials DOD has fielded or plans to field PACS that connect to IMESA at all domestic installations, only the Air Force and DLA have monitored PACS use at their installations. The Army, the Navy, and the Marine Corps at more than 100 installations have not monitored the use of PACs because, as stated by officials, there is not a requirement to do so. As a result, these components do not have the data necessary to evaluate PACS effectiveness and inform risk-based decisions regarding PACS use to safeguard personnel and mission-critical, high-value installation assets. Further, DOD component and installation officials told us about their dissatisfaction with the time it takes to resolve DBIDS' technical issues. Although the Army has developed performance measures and associated goals for its helpdesk that have improved the ability to resolve technical issues and overall AIE operational availability, DMDC has not. Without such performance measures and associated goals, DMDC is unable to systematically evaluate how well DBIDS is performing and address underlying issues negatively affecting DBIDS' operational availability.

Recommendations for Executive Action

We are making the following five recommendations to the Department of Defense:

The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence requires that DOD components (including the military departments and DLA) monitor the use of PACS at their installations. (Recommendation 1)

The Secretary of the Army should ensure that the Office of Provost Marshal General monitors the use of PACS at Army installations. (Recommendation 2)

The Secretary of the Navy should ensure that the Commander, Navy Installations Command, monitors the use of PACS at Navy installations. (Recommendation 3)

The Secretary of the Navy, in coordination with the Commandant of the Marine Corps, should ensure that the Commander, Marine Corps

Installations Command, monitors the use of PACS at Marine Corps installations. (Recommendation 4)

The Secretary of Defense should ensure that the Under Secretary of Defense for Personnel and Readiness develops appropriate performance measures and associated goals for the timely resolution of DBIDS technical issues to facilitate improved PACS performance. (Recommendation 5)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for comment. In its written comments, reproduced in appendix II, DOD concurred with our five recommendations and identified actions that it was taking or planned to take to implement our recommendations. Regarding our second recommendation, DOD concurred with that recommendation to monitor the use of PACS at Army installations, and on the basis of the department's written comments we modified the recommendation to indicate that the Army Office of the Provost Marshal General is responsible for monitoring the use of PACS at Army installations. DOD also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and the Under Secretary of Defense for Intelligence. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9627 or maurerd@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix III.

Diana Maurer
Director
Defense Capabilities and Management

List of Committees

The Honorable James M. Inhofe
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable John Boozman
Chairman
The Honorable Brian Schatz
Ranking Member
Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Committee on Appropriations
United States Senate

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Debbie Wasserman Schultz
Chairwoman
The Honorable John Carter
Ranking Member
Subcommittee on Military Construction, Veterans Affairs and Related Agencies
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

In this report we (1) describe actions the Department of Defense (DOD) has taken to develop guidance on physical access to domestic installations and to field physical access control systems (PACS) at these installations, (2) evaluate the extent to which DOD components have monitored the use of fielded PACS at these installations, and (3) evaluate the extent to which DOD has implemented an approach for addressing PACS technical issues and assessing associated performance.

This report is a public version of a sensitive report that we issued on May 31, 2019.[1] The sensitive report included an objective related to the extent to which security forces at various DOD domestic installations used fielded PACS. DOD deemed a significant portion of the information related to this objective to be sensitive, necessitating protection from public disclosure. This public report omits information related to our observations of PACS use at these installations and the risks associated with not using PACS. As a result of this omission, we updated the wording of the second objective to focus on DOD components' efforts to monitor the use of fielded PACS at installations. Although the second objective and the information associated with it in this public report is more limited, we relied on the same methodology to support our findings and the excluded information does not impact our recommendations. The first and third objectives in this report are the same as in the sensitive report and use the same methodology as in the sensitive report. DOD deemed some of the detailed information presented in conjunction with the third objective to be sensitive, necessitating protection from public disclosure. As a result, this public report omits specific details regarding the technical issues of PACs.

This report focuses on physical access controls at authorized access control points at DOD's domestic installations that are owned and operated by the Army, the Navy, the Air Force, the Marine Corps, and the

[1]GAO, *DOD Installations: Monitoring the Use of Physical Access Control Systems Could Reduce Risks to Personnel and Assets*, GAO-19-316SU (Washington, D.C.: May 31, 2019).

Defense Logistics Agency (DLA).[2] We did not consider actions DOD has taken to prevent unauthorized access to its domestic installations by means such as tunneling under or climbing over perimeter barriers.

For objective one, we analyzed key Office of the Under Secretary of Defense for Intelligence (OUSD(I)) and DOD component policies outlining physical access control requirements. The key guidance documents we analyzed are listed in table 2.

[2]By "domestic installations," we are referring to active-duty DOD installations in the continental United States. We refer to the Army, the Navy, the Marine Corps, the Air Force, and DLA collectively as the "DOD components." DOD Manual 5200.08 Volume 3 defines "installation" as the grounds of, but not buildings on, a base, camp, post, station, yard, center, homeport facility for any ship, or other activity under DOD jurisdiction, including any leased facility located within the United States that has a perimeter barrier (such as a fence line or wall), one or more access control points, and a method for processing visitors, except for any facility used primarily for civil works, rivers and harbors projects, or flood control projects.

Table 2: Department of Defense (DOD) Guidance That We Analyzed

- DOD Manual 5200.08 Volume 3, *Physical Security Program: Access to DOD Installations* (Jan. 2, 2019)
- DOD Instruction 5525.19, *DOD Identity Matching Engine for Security and Analysis (IMESA) Access to Criminal Justice Information (CJI) and Terrorist Screening Databases (TSDB)* (May 4, 2016) (incorporating change 1, effective June 29, 2018)
- DOD Regulation 5200.08-R, *Physical Security Program* (Apr. 9, 2007) (incorporating change 1, effective May 27, 2009)
- DOD Instruction 5200.08, *Security of DOD Installations and Resources and the DOD Physical Security Review Board (PSRB)* (Dec. 10, 2005) (incorporating change 3, effective Nov. 20, 2015)
- Army Regulation 190-13, *The Army Physical Security Program* (Feb. 25, 2011) (effective Mar. 27, 2011)
- Air Force Manual 31-113, *Installation Perimeter Access Control* (Feb. 2, 2015) (incorporating changes from Air Force Guidance Memorandum 2018-01, effective Apr. 4, 2018)
- Commander Navy Installations Command Instruction 5530.14A, *Commander Navy Installations Command Ashore Protection Program* (June 6, 2016) (change transmittal 2)
- Marine Corps Installation Command Policy, *MCICOM Installation Physical Access Control Policy* (September 2015)
- Marine Corps Order 5530.14A, *Marine Corps Physical Security Program Manual* (June 5, 2009)
- Defense Logistics Agency (DLA) Instruction 5200.08 Volume 1, *Physical Security Program* (July 21, 2017)
- Defense Logistics Agency (DLA) Manual 5200.08-V1, *Physical Security* (July 15, 2016)

Source: DOD. | GAO-19-649

Additionally, we interviewed officials from OUSD(I), the Joint Staff, each of the DOD components, and the U.S. Northern Command to discuss the guidance documents and any efforts to update, revise, or draft new guidance on the use of installation PACS. We also reviewed DOD component documentation and interviewed OUSD(I) and DOD component officials to determine the extent to which PACS was fielded at domestic installations and to identify ongoing efforts to field PACS at additional domestic installations. Finally, we interviewed DOD officials to identify any planned future enhancements to PACS and the Identify Matching Engine for Security and Analysis (IMESA).

For our second objective, we focused on individuals seeking unescorted access to DOD domestic installations. We reviewed and analyzed OUSD(I), DOD component, and installation-specific guidance on the use

and monitoring of PACS.[3] We conducted site visits to six domestic installations to meet with installation command and security force officials to discuss their experiences using PACS and to observe their use of PACS. We then compared the guidance and our observations with *Standards for Internal Control in the Federal Government* for monitoring activities, which states that management should obtain data on a timely basis so that they can be used for effective monitoring.[4] Although findings from these six installations are not generalizable to all DOD domestic installations, they are illustrative of how PACS are used, and more generally, how installation access is controlled.

In selecting the six installations to visit we considered installation ownership to ensure that we included an installation from each DOD component, geographic proximity among installations, and the type of PACS used by the installation. We also visited an installation where no PACS was installed. We limited our site selection to active-duty installations in the continental United States. Based on this methodology we visited Fort Stewart, Georgia; Moody Air Force Base, Georgia; Naval Station Mayport, Florida; Marine Corps Support Facility Blount Island, Florida; Tobyhanna Army Depot, Pennsylvania; and DLA Distribution Center Susquehanna, Pennsylvania.

For our third objective, we reviewed DOD user agreements to determine the support agreement terms, requirements, and responsibilities for addressing PACS technical issues. We analyzed DOD component data on the number and type of Defense Biometric Identification System (DBIDS) helpdesk technical issues reported from January 2016 through July 2018, and compared the data with provisions in the user agreements that discuss the PACS helpdesk.[5] We also compared the steps the Army and DMDC have taken or planned to address helpdesk technical issues with *Standards for Internal Control in the Federal Government* for

[3]We also reviewed OUSD(I) and DOD component guidance that govern access control for standalone facilities and enclaves, but we did not evaluate the facilities' and enclaves' use of PACS. According to OUSD(I) officials, "standalone facilities" are access-controlled structures outside of an installations but are that are under the authority, direction, and control of DOD. "Enclaves" are areas with more restrictive access controls within an installation, such as an airfields or operations centers, that are under the authority, direction, and control of DOD.

[4]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: September 2014).

[5]We focused on DBIDS since that is the PACS the majority of the DOD components use.

developing performance measures, which states that management should establish performance measures and indicators.[6] We interviewed officials from DOD components and the installations we visited to discuss their experiences with PACS helpdesks, and their views on the performance and reliability of PACS. We assessed the reliability of the helpdesk technical issue data by interviewing knowledgeable officials about the data and by testing the raw data to determine the accuracy of the summary data provided by DOD. Additionally, we collected and analyzed the raw data to determine whether calculations were made correctly. We determined that the data were sufficiently reliable for our understanding the number and types of PACS technical issues.

To address our three reporting objectives, we met with officials from the DOD organizations listed in table 3.

[6]GAO-14-704G.

Table 3: Department of Defense (DOD) Organizations We Met with During Our Audit

Office of the Secretary of Defense • Office of the Under Secretary of Defense for Intelligence • Office of the Under Secretary of Defense for Personnel and Readiness
Joint Staff • Operations Directorate (J3) • Force Structure, Resources, and Assessment Directorate (J8)
U.S. Army • Army Installation Management Command • Office of the Provost Marshal General, Physical Security Branch • Army Program Executive Office for Intelligence Electronic Warfare & Sensors • Office of the Product Manager for Force Protection Systems • Army Audit Agency • Tobyhanna Army Depot, Pennsylvania • Fort Stewart Army Base, Georgia
U.S. Navy • Office of the Assistant Secretary of the Navy for Energy, Installations and Environment • Office of the Deputy Under Secretary of the Navy, Policy and Strategy • Navy Installations Command • Naval Station Mayport, Florida
U.S. Air Force • Logistics, Engineering and Force Protection Directorate (A4) • Air Force Security Forces Center • Moody Air Force Base, Georgia
U.S. Marine Corps • Office of the Deputy Commandant for Plans, Policies and Operations • Marine Corps Installations Command • Office of the Deputy Commandant for Installations and Logistics • Marine Corps Support Facility Blount Island, Florida
U.S. Northern Command • Homeland Defense and Protection Division (J34)
Defense Logistics Agency • Installation Support, Security and Emergency Services • Installation Support, Process Management • Information Operations Directorate (J6) • Defense Distribution Center Susquehanna, Pennsylvania

Source: GAO. | GAO-19-649

We conducted this performance audit from February 2018 to August 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with DOD from July 2019 to August 2019 to prepare this public version of the original sensitive report. This public version was also prepared in accordance with these standards.

Appendix II: Comments from the Department of Defense

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

INTELLIGENCE

MAY - 7 2019

Ms. Diana Maurer
Director, Defense Capabilities Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Maurer:

This is the Department of Defense response to the GAO Draft Report, GAO-19-316, "DOD INSTALLATIONS: Monitoring the Use of Physical Access Control Systems Could Reduce Risk to Personnel and Assets," dated May 2019 (GAO Code 102634). Detailed comments on the report recommendations are enclosed. Thank you for the opportunity to provide comments on this draft report.

Sincerely,

Garry P. Reid
Director for Defense Intelligence
(Counterintelligence, Law Enforcement, & Security)

Enclosure:
As stated

GAO DRAFT REPORT DATED MAY 1, 2019
GAO-19-316 (GAO CODE 102634)

"DEFENSE INSTALLATIONS: MONITORING THE USE OF PHYSICAL ACCESS CONTROL SYSTEMS COULD REDUCE RISK TO PERSONNEL AND ASSETS"

DEPARTMENT OF DEFENSE COMMENTS IN RESPONSE TO THE GAO RECOMMENDATIONS

GAO RECOMMENDATION 1: The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence requires that DoD Components (including the military services and the Defense Logistics Agency) monitor the use of physical access control systems (PACS) at their installations.

DoD RESPONSE: DoD concurs with the recommendation requiring monitoring of the use of PACS at DoD installations. DoD is currently drafting DoD Manual 5200.08 Volume 1, which will outline overall requirements for the implementation of DoD's physical security program, and we will address monitoring the use of PACS in this new manual volume. We expect this new manual volume will enter formal coordination in summer 2020.

GAO RECOMMENDATION 2: The Secretary of the Army should ensure that the Army's Acquisition Corps, Product Manager for Force Protection Systems monitors the use of PACS at Army installations.

DoD RESPONSE: DoD concurs with the recommendation, but the Office of the Provost Marshal General (OPMG), not the Acquisition Corps, is responsible for implementing the recommended monitoring of PACS use at Army installations. OPMG agrees that monitoring could help identify where risk is being incurred by installations not meeting the standard in using their PACS.

OPMG further recommends adding the following language to the bullet on page six describing the capabilities of Army's Automated Installation Entry (AIE) system: "AIE has the capability to conduct 'in-lane' vetting and registration in IMESA for visitors who have not previously been registered. This ability eliminates the requirement for the visitors to process through the Visitor's Center for initial vetting and IMESA registration. This in-lane initial vetting and IMESA registration takes approximately 30 seconds by using the Nlets system to check the National Crime Information Center and Interstate Identification Index for criminal history, terrorist alerts, and active warrants from Federal and state databases."

GAO RECOMMENDATION 3: The Secretary of the Navy should ensure that the Commander, Navy Installations Command (CNIC) monitors the use of PACS at Navy installations.

DoD RESPONSE: DoD concurs with the recommendation and will take steps to monitor the use of PACS at Navy installations. The Navy will accomplish this by requiring PACS usage in

CNIC's upcoming access control instruction. CNIC will also collect data on PACS use and the number of credentials scanned at Navy installations to effectively brief installation commanders on the risks associated with not using the PACS at their installations.

GAO RECOMMENDATION 4: The Secretary of the Navy, in coordination with the Commandant of the Marine Corps, should ensure that the Commander, Marine Corps Installations Command monitors the use of PACS at Marine Corps installations.

DoD RESPONSE: DoD concurs with the recommendation and the Secretary of the Navy, through the Deputy Under Secretary of the Navy, has directed actions that implement this recommendation. Beginning February 2019, Marine Corps statistics regarding PACS use and card approval, denial, and warning information are submitted monthly.

GAO RECOMMENDATION 5: The Secretary of Defense should ensure that the Under Secretary of Defense for Personnel and Readiness develops appropriate performance measures and associated goals for the timely resolution of DBIDS technical issues to facilitate improved PACS performance.

DoD RESPONSE: DoD concurs with the recommendation.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Diana Maurer, (202) 512-9627 or maurerd@gao.gov

Staff Acknowledgments

In addition to the contact name above, GAO staff who made key contributions on this report include Brian Lepore, Director (retired); Jason Bair, Acting Director; Marc Schwartz, Assistant Director; Shawn Arbogast, Analyst-in-Charge; Jamilah Moon; Richard Hung; Mae Jones; Amie Lesser; Serena Lo; Amber Lopez Roberts; and Carter Stevens.

Appendix IV: Accessible Data

Agency Comment Letter

Accessible Text for Appendix II Comments from the Department of Defense

Page 1

MAY - 7 2019

Ms. Diana Maurer

Director, Defense Capabilities Management

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Dear Ms. Maurer:

UAY - 7 2019

This is the Department of Defense response to the GAO Draft Report, GAO-19-316, "DOD INSTALLATIONS: Monitoring the Use of Physical Access Control Systems Could Reduce Risk to Personnel and Assets," dated May 2019 (GAO Code 102634). Detailed comments on the report recommendations are enclosed. Thank you for the opportunity to provide comments on this draft report.

Sincerely,

Garry P. Reid

Director for Defense Intelligence (Counterintelligence, Law Enforcement, & Security)

Enclosure:

As stated

Page 2

GAO RECOMMENDATION 1: The Secretary of Defense should ensure that the Under Secretary of Defense for Intelligence requires that DoD Components (including the military services and the Defense Logistics Agency) monitor the use of physical access control systems (PACS) at their installations.

DoD RESPONSE: DoD concurs with the recommendation requiring monitoring of the use of PACS at DoD installations. DoD is currently drafting DoD Manual 5200.08 Volume 1, which will outline overall requirements for the implementation ofDoD's physical security program, and we will address monitoring the use of PACS in this new manual volume. We expect this new manual volume will enter formal coordination in summer 2020.

GAO RECOMMENDATION 2: The Secretary of the Army should ensure that the Army's Acquisition Corps, Product Manager for Force Protection Systems monitors the use of PACS at Army installations.

DoD RESPONSE: DoD concurs with the recommendation, but the Office of the Provost Marshal General (OPMG), not the Acquisition Corps, is responsible for implementing the recommended monitoring of PACS use at Army installations. OPMG agrees that monitoring could help identify where risk is being incurred by installations not meeting the standard in using their PACS.

OPMG further recommends adding the following language to the bullet on page six describing the capabilities of Army's Automated Installation Entry (AIE) system: "AIE has the capability to conduct 'in-lane' vetting and registration in IMESA for visitors who have not previously been registered. This ability eliminates the requirement for the visitors to process through the Visitor's Center for initial vetting and IMESA registration. This in-lane initial vetting and IMESA registration takes approximately 30 seconds by using the Nlets system to check the National Crime Information Center and Interstate Identification Index for criminal history, terrorist alerts, and active warrants from Federal and state databases."

GAO RECOMMENDATION 3: The Secretary of the Navy should ensure that the Commander, Navy Installations Command (CNIC) monitors the use of PACS at Navy installations.

DoD RESPONSE: DoD concurs with the recommendation and will take steps to monitor the use of PACS at Navy installations. The Navy will accomplish this by requiring PACS usage in

Page 3

CNIC's upcoming access control instruction. CNIC will also collect data on PACS use and the number of credentials scanned at Navy installations to effectively brief installation commanders on the risks associated with not using the PACS at their installations.

GAO RECOMMENDATION 4: The Secretary of the Navy, in coordination with the Commandant of the Marine Corps, should ensure that the Commander, Marine Corps Installations Command monitors the use of PACS at Marine Corps installations.

DoD RESPONSE: DoD concurs with the recommendation and the Secretary of the Navy, through the Deputy Under Secretary of the Navy, has directed actions that implement this recommendation. Beginning February 2019, Marine Corps statistics regarding PACS use and card approval, denial, and warning information are submitted monthly.

GAO RECOMMENDATION 5: The Secretary of Defense should ensure that the Under Secretary of Defense for Personnel and Readiness develops appropriate performance measures and associated goals for the timely resolution of DBIDS technical issues to facilitate improved PACS performance.

DoD RESPONSE: DoD concurs with the recommendation.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548