August 2019

DOD INSTALLATIONS

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

GAO Highlights

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

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

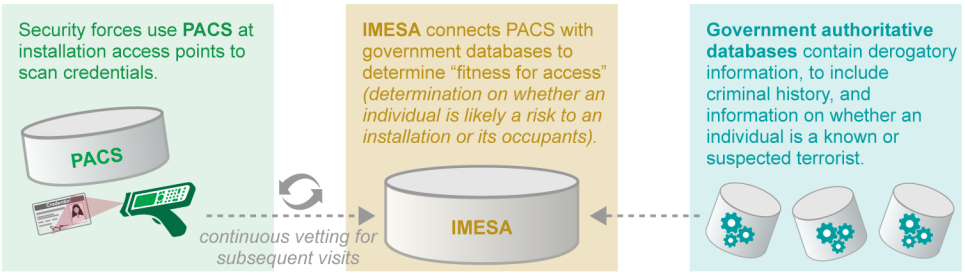
GAO made five recommendations, including that DOD monitor installations' use of PACS and develop appropriate performance measures and goals for resolving technical issues to improve PACS performance. DOD concurred with GAO's recommendations.

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.