June 2024

PERSONNEL VETTING

DOD Needs to Enhance Cybersecurity of Background Investigation Systems

GAO Highlights

Highlights of GAO-24-106179, a report to congressional committees

Why GAO Did This Study

In the wake of a 2015 OPM breach that compromised sensitive data on over 22 million federal employees and contractors, DCSA later assumed responsibility for conducting background investigation operations for most executive branch agencies.

House Report 117-118 includes a provision for GAO to evaluate the cybersecurity of DCSA's background investigation systems. GAO assessed the extent to which DCSA (1) planned for cybersecurity controls for selected background investigation systems and (2) implemented privacy controls for these systems.

GAO selected three DCSA systems and three OPM legacy systems critical to background investigation operations. GAO (1) reviewed policies, processes, and documentation for these systems and (2) interviewed agency officials regarding the planning and management of cybersecurity risks and selected privacy controls. GAO also has ongoing work assessing DCSA's implementation of technical controls for background investigation systems. It will be published in a future report with limited distribution.

What GAO Recommends

GAO is making a total of 13 recommendations to DOD on fully implementing risk management planning steps, selecting appropriate security controls using current guidance, fully implementing privacy controls, and establishing oversight processes to help ensure required tasks and controls are implemented. DOD concurred with 12 of 13 recommendations and non-concurred with one. GAO maintains that all recommendations are warranted.

View GAO-24-106179. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov and Alissa H. Czyz, (202) 512-3058 or czyza@gao.gov.

What GAO Found

To conduct background investigations, the Department of Defense's (DOD) Defense Counterintelligence and Security Agency (DCSA) currently uses a combination of recently developed DOD National Background Investigation Services systems and legacy systems formerly owned by the Office of Personnel Management (OPM). In considering the cybersecurity risks of these systems, DCSA did not fully address all planning steps of DOD's risk management framework (see figure).

Extent to Which Defense Counterintelligence and Security Agency Addressed DOD's Planning-Related Risk Management Steps for Selected Background Investigation Systems as of December 2023

Sources: GAO (icons and analysis of Department of Defense [DOD] guidance); colorlife/stock.adobe.com (illustration). | GAO-24-106179

Note: DOD's implementation-related Risk Management Steps are to (3) establish an implementation approach, (4) assess security controls, (5) authorize the systems, and (6) monitor security controls.

- **Prepare the organization and systems:** Of the 16 tasks required by this step in DOD's risk management framework, DCSA fully addressed 11, partially addressed two, and did not address three. For example, the agency has not fully defined and prioritized security and privacy requirements, nor has it performed organizational and system-level risk assessments.
- **Categorize the systems:** DCSA appropriately categorized the six reviewed systems as high impact risks**.**
- **Select security controls:** DCSA selected baseline security controls for the six systems but used an outdated version of government-wide guidance as the source for the control selections. Specifically, version five of applicable National Institute for Standards and Technology guidance was issued in 2020. However, DCSA continues to use version four. Among the changes in version five are two new categories of controls on personally identifiable information and supply chain management, raising the number of control categories from 18 to 20.

Regarding privacy, DCSA partially implemented controls on developing policies and procedures, delivering training, defining and reviewing the types of events to log, and assessing controls and risks. The agency lacks an oversight process to help ensure that appropriate privacy controls are fully implemented. Until DCSA establishes such an oversight process and fully implements privacy controls, it unnecessarily increases the risks of disclosure, alteration, or loss of sensitive information on its background investigation systems.