GAO@100 Highlights

Highlights of GAO-21-278, a report to the Committee on Armed Services, House of Representatives

Why GAO Did This Study

In November 2018 DOD's Survivable Logistics Task Force examined current and emerging threats to DOD logistics, including cybersecurity threats. The task force concluded that DOD's inventory management systems were potentially vulnerable to cyberattacks, and that DOD did not have corrective action plans to mitigate the potential risks posed by associated vulnerabilities.

House Report 116-120, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2020, included a provision for GAO to evaluate DOD's efforts to manage cybersecurity risks to the DOD supply chain. GAO's report determines the extent to which DLA has implemented risk management steps to address cybersecurity risks to its inventory management systems.

GAO selected six systems that DLA officials deemed critical to inventory management operations. GAO reviewed documents, analyzed data, and interviewed officials to determine whether DLA fully addressed, partially addressed, or did not address DOD steps for cybersecurity risk management.

What GAO Recommends

GAO is making five recommendations for DLA to address shortfalls in its critical inventory management systems' adherence to DOD cybersecurity risk management steps. DLA agreed with two and partially agreed with three recommendations. GAO continues to believe all its recommendations are still warranted.

View GAO-21-278 report. For more information, contact Diana Maurer at (202) 512-9627 or MaurerD@gao.gov or Vijay A D'Souza at 202-512-6240 or Dsouzav@gao.gov

June 2021

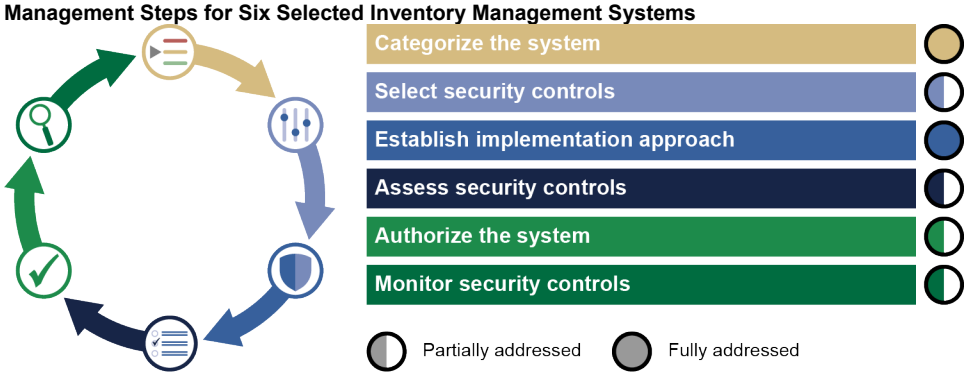
DEFENSE CYBERSECURITY

Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems

What GAO Found

For six selected inventory management systems that support processes for procuring, cataloging, distributing, and disposing of materiel, the Defense Logistics Agency (DLA) fully addressed two of the Department of Defense's (DOD) six cybersecurity risk management steps and partially addressed the other four. Specifically, the agency categorized the systems based on risk and established an implementation approach for security controls. However, it only partially addressed the four risk management steps of selecting, assessing, authorizing, and monitoring security controls (see figure).

Extent to Which the Defense Logistics Agency Addressed the Department of Defense's Risk Management Steps for Six Selected Inventory Management Systems



Source: GAO analysis of Defense Logistics Agency information management inventory systems. | GAO-21-278

- **Select security controls**: DLA selected specific security controls, but it did not develop system-level monitoring strategies to assess the effectiveness of selected security controls for three of the six systems GAO assessed. DOD's risk management framework requires components to develop a system-specific monitoring strategy during the security control selection step.

- **Assess security controls**: DLA assessed the security controls for the six selected inventory management systems, but its assessment procedures lacked approvals, as required. As a result, GAO found that DLA's assessment plans lacked essential details and missed opportunities for risk-based decisions.

- **Authorize the system**: DLA authorized the selected systems, but it did not report complete and consistent security and risk assessment information to support decisions. GAO found that DLA had not established a process for program offices to review authorization documentation prior to submitting packages to the authorizing official.

- **Monitor security controls**: DLA did not consistently monitor the remediation of identified security weaknesses across its six inventory management systems. As a result, GAO found that 1,115 of the 1,627 corrective action plans (69 percent) for the six systems did not complete intended remediation within DLA's required time frame of 365 days or less--they were ongoing for an average of 485 days.

Until DLA addresses the identified deficiencies, the agency's management of cyber risks for critical systems will be impeded and potentially pose risks to other DOD systems that could be accessed if DLA's systems are compromised.