CYBERSECURITY

DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program

What GAO Found

Selected agencies—the Federal Aviation Administration, Indian Health Services, and Small Business Administration—had generally deployed tools intended to provide cybersecurity data to support the Department of Homeland Security’s (DHS) Continuous Diagnostics and Mitigation (CDM) program. As depicted in the figure, the program relies on automated tools to identify hardware and software residing on agency networks. This information is aggregated and compared to expected outcomes, such as whether actual device configuration settings meet federal benchmarks. The information is then displayed on an agency dashboard and federal dashboard.

Continuous Diagnostics and Mitigation Program Data Flow from Agencies to the Federal Dashboard

However, while agencies reported that the program improved their network awareness, none of the three agencies had effectively implemented all key CDM program requirements. For example, the three agencies had not fully implemented requirements for managing their hardware. This was due in part to contractors, who install and troubleshoot the tools, not always providing unique identifying information. Accordingly, CDM tools did not provide an accurate count of the hardware on their networks. In addition, although most agencies implemented requirements for managing software, they were not consistently comparing configuration settings on their networks to federal core benchmarks intended to maintain a standard level of security.

The agencies identified various challenges to implementing the program, including overcoming resource limitations and not being able to resolve problems directly with contractors. DHS had taken numerous steps to help manage these challenges, including tracking risks of insufficient resources, providing forums for agencies to raise concerns, and allowing agencies to provide feedback to DHS on contractor performance.

What GAO Recommends

GAO is making six recommendations to DHS, including to ensure that contractors provide unique hardware identifiers; and nine recommendations to the three selected agencies, including to compare configurations to benchmarks. DHS and the selected agencies concurred with the recommendations.