

GAO Highlights

Highlights of [GAO-23-105466](#), a report to congressional requesters

Why GAO Did This Study

Given the ever-increasing cyber threat landscape, the federal government has initiatives underway intended to protect agency IT. One such initiative, a zero trust architecture, is based on the concept that no actor operating outside or within an organization's network should be trusted.

The U.S. Secret Service, a component of the Department of Homeland Security (DHS), relies heavily on the use of IT to support its protection and financial investigations mission. GAO was asked to review cybersecurity at the agency. The objective of this report was to evaluate Secret Service's implementation of a zero trust architecture.

To do so, GAO reviewed the activities associated with four milestones the agency had developed with the intent of supporting a zero trust architecture. GAO compared Secret Service plans to OMB requirements and industry best practices.

GAO also reviewed configuration settings and interviewed agency officials about the milestones. GAO reviewed additional actions that the agency either had underway, or intended to take, to determine if the actions would meet OMB's requirements.

What GAO Recommends

GAO is making two recommendations to the Secret Service, including to transition to a more advanced internet protocol for its public-facing systems and to update its zero trust architecture implementation plan. DHS, on behalf of Secret Service, concurred with the recommendations.

View [GAO-23-105466](#). For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov.

November 2022






CYBERSECURITY

Secret Service Has Made Progress Toward Zero Trust Architecture, but Work Remains

What GAO Found

A zero trust architecture is a set of cybersecurity principles stating that organizations must verify everything that attempts to access their systems and services. These principles cover five pillars (see figure).

Cybersecurity and Infrastructure Security Agency Pillars of Zero Trust Architecture

 Identity	Enforcing access controls to confirm the identity of all users. Ensuring that the right users have the right access at the right time.
 Device	Compiling and maintaining ongoing inventories of all devices connected to the network. Ensuring that devices are secure to prevent, detect, and respond to unauthorized access to an enterprise's resources.
 Network	Encrypting open communication channels that are used to transport messages on the network. Segmenting those channels into isolated environments.
 Applications and Workloads	Securing and managing applications by performing rigorous internal and external testing and decreasing reliance on network security.
 Data	Protecting data on devices, networks, and applications by implementing enterprise-wide logging and information sharing.

Source: GAO analysis of the Cybersecurity and Infrastructure Security Agency's *Zero Trust Maturity Model Version 1.0* (draft) and other relevant federal policies and guidance; images: lembervector/stock.adobe.com. | GAO-23-105466

The U.S. Secret Service developed an implementation plan for four milestones intended to support a zero trust architecture. The milestones are to (1) perform a self-assessment of the agency's IT environment against federal guidance, (2) implement cloud service offerings from a vendor, (3) achieve maturity in event logging, and (4) transition the agency's IT infrastructure to a more advanced internet protocol. Secret Service completed a self-assessment, and made progress in implementing cloud services and achieving maturity in event logging. In addition, the agency had a plan to implement a more advanced internet protocol, but had not met longstanding Office of Management and Budget (OMB) requirements for public-facing systems. By transitioning to this protocol, the agency can leverage additional security features.

Secret Service had additional efforts underway that could address actions specified in OMB's zero trust strategy issued in January 2022. However, because Secret Service developed its implementation plan before OMB issued the strategy, the plan's milestones do not cover all of OMB's required actions. Further, Secret Service has not updated its implementation plan to reflect these additional efforts. Doing so would provide agency management with a comprehensive and unified view of disparate activities associated with the zero trust architecture transition process.