GAO
Highlights

Highlights of GAO-24-106343, a report to congressional committees

April 2024

CYBERSECURITY

Implementation of Executive Order Requirements Is Essential to Address Key Actions

Why GAO Did This Study

For more than 25 years, GAO has identified information security as a high-risk area. During this period, the threat of cyber-based attacks on IT systems has continued to grow. In 2021, the President issued Executive Order 14028 to enhance federal resilience in protecting IT systems. The order contains requirements for federal agencies to improve their ability to identify, protect against, and respond to malicious cyber threats.

The Federal Information Security Modernization Act of 2014 includes a provision for GAO to periodically report on agencies' progress in improving their cybersecurity practices. This report examines the extent to which (1) agencies have implemented Executive Order 14028 leadership and oversight-related requirements and (2) the order has addressed federal cybersecurity challenges.

To do so, GAO identified government-wide leadership and oversight requirements in the order and the key agencies required to perform them. GAO then reviewed the agencies' implementation of those requirements. GAO also compared challenges identified in its work and in discussions with federal CISOs against the content of the order to determine whether they were addressed.

What GAO Recommends

GAO is making two recommendations to DHS and three to OMB to fully implement the order's requirements. DHS agreed with recommendations to further define critical software and improve operations of the Cyber Safety Review Board. OMB stated it had no comments on GAO's report.

View GAO-24-106343. For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov.

What GAO Found

Among its 115 provisions, the order contains 55 leadership and oversight requirements (actions to assist or direct the federal agencies in implementing the order). The three key agencies primarily responsible for the implementation of these requirements are the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency, the National Institute of Standards and Technology, and the Office of Management and Budget (OMB). These agencies fully completed 49 of the 55 requirements, partially completed five, and one was not applicable (see table below). Completing these requirements would provide the federal government with greater assurance that its systems and data are adequately protected.

Progress in Implementing Executive Order 14028 Leadership and Oversight Requirements, as of March 2024

	Number of requirements that are:			
Executive Order Section	Fully complete	Partially complete	Not complete	Not applicable
Removing Barriers to Sharing Threat Information	6	1	—	—
Modernizing Federal Government Cybersecurity	8	—	—	—
Enhancing Software Supply Chain Security	16	1	—	—
Establishing a Cyber Safety Review Board	6	1	—	—
Standardizing Playbook for Responding to Cybersecurity Vulnerabilities and Incidents	4	—	—	1
Improving Detection of Cybersecurity Vulnerabilities and Incidents	7	1	—	—
Improving the Federal Government's Investigative and Remediation Capabilities	2	1	—	—
Total	49	5	—	1

Legend: fully complete = those where the actions required are complete; partially complete = those where GAO judged significant, but not complete, progress to be made in completing a requirement; not complete = those where the progress made toward completion was minimal and not significant. The symbol "—" indicates that no requirements received this score.

Source: GAO analysis of documentation from the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency; the National Institute of Standards and Technology; and the Office of Management and Budget. | GAO-24-106343

GAO's High-Risk Series identified ten action areas critical to addressing the nation's cybersecurity challenges. The order's requirements directly address five of these ten critical action areas, while each of the other five could be addressed by other recently-issued strategies, frameworks, and guidance. For example, the cyber workforce and critical infrastructure action areas could potentially be addressed by the *National Cyber Workforce Strategy* and *National Cybersecurity Strategy*, if implemented effectively. In addition to the ten action areas, six federal chief information security officers (CISO) identified additional cyber issue areas they considered to be challenging, such as uncertainty in cyber funding, creating a culture that prioritizes cybersecurity as an essential mission component, and focus on cyber compliance versus cyber resilience. The order's requirements also address each of these additional cyber issue areas identified by CISOs. For example, the order addresses uncertainties in cyber funding by requiring OMB to assist agencies in having sufficient resources to implement its requirements.