September 2023

CYBERSECURITY

State Needs to Expeditiously Implement Risk Management and Other Key Practices

GAO Highlights

Highlights of GAO-23-107012, a report to congressional requesters

Why GAO Did This Study

The security of State's IT systems is vital to promoting an open, interoperable, and reliable information and communications infrastructure in the department.

GAO was asked to review State's cybersecurity practices. This report assesses the extent to which (1) State has implemented a cybersecurity risk management program; (2) State has a process and supporting infrastructure to detect, respond to, and recover from cybersecurity incidents; and (3) State's Chief Information Officer (CIO) is able to secure its IT systems department-wide.

To conduct this work, GAO reviewed federal laws and guidance and compared them to department policies. GAO also analyzed samples of IT risk, incident response, and configuration data for selected enterprise-wide systems and 16 embassies and consular locations. Additionally, GAO interviewed State officials from the Bureau of Information Resource Management and the Bureau of Diplomatic Security with primary responsibility for managing and securing State's IT systems and networks. GAO also met with high-level officials at the Bureau of Consular Affairs, given that it operates more IT systems than any other bureau.

This is a public version of a sensitive report with limited distribution. In response to a request from State officials, GAO excluded from this public report information deemed sensitive, such as specific post locations, system names, and technologies as well as a specific weakness.

View GAO-23-107012. For more information, contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov or Latesha Love-Grayer at (202) 512-4409 or lovegrayerl@gao.gov.

What GAO Found

The Department of State has documented a cybersecurity risk management program that meets federal requirements. Specifically, the department has identified risk management roles and responsibilities and developed a risk management strategy. However, State has not fully implemented its program to identify and monitor risk to assets and the information maintained on its systems, as shown in the figure below.

Examples of State's Progress in Implementing Its Cybersecurity Risk Management Program

- ✓ **Identified risk management roles and responsibilities**
- ✓ **Developed a cyber risk management strategy**
- ✗ Mitigated department-wide cybersecurity risks
- ✗ Conducted required bureau-level risk assessments
- ✗ Completed the authorization to operate process for its 494 information systems, including high value assets (completed 44%)
- ✗ Implemented a department-wide continuous monitoring program

✓ Implemented ✗ Not implemented

Source: GAO analysis of Department of State documentation. | GAO-23-107012

Until the department implements required risk management activities, it lacks assurance that its security controls are operating as intended. Moreover, State is likely not fully aware of information security vulnerabilities and threats affecting mission operations.

State's incident response processes for detecting, responding to, and recovering from cybersecurity incidents generally align with federal guidance by requiring the department to establish an incident handling capability for its information systems. For example, State's Cyber Incident Response Team and other units within its Monitoring and Incident Response Division provide the capability to identify active and potential threats to the department's network security 24 hours a day, 7 days a week.

However, the department has not fully implemented processes that support its incident response program. For example, State has not fully updated and tested information system contingency plans to ensure continuity of operations nor configured its centralized inventory management database to identify asset inventory information from all available data sources.

Further, State has not adequately secured its IT infrastructure to support its incident response program. This includes replacing the 23,689 hardware systems and 3,102 occurrences of network and server operating system software installations that have reached end-of-life. Certain installations of operating system software had reached end-of-life over 13 years ago.

What GAO Recommends

GAO is making 15 recommendations to State, including that the Secretary of State

- develop plans to mitigate vulnerabilities that State previously identified,
- conduct bureau-level risk assessments for the 28 bureaus that owned information systems that GAO reviewed,
- ensure that its information systems have valid authorizations to operate in accordance with department policies and federal guidance,
- ensure that the CIO has access to assets at bureaus and posts to continuously monitor for threats and vulnerabilities that may affect mission operations,
- ensure that all system contingency plans for high value assets are tested annually as required by department policies, and
- direct the CIO to update an October 2020 matrix to better ensure compliance with applicable department policies and federal guidance.

State concurred with all 15 recommendations to address cybersecurity weaknesses and provided technical comments, which were incorporated as appropriate.

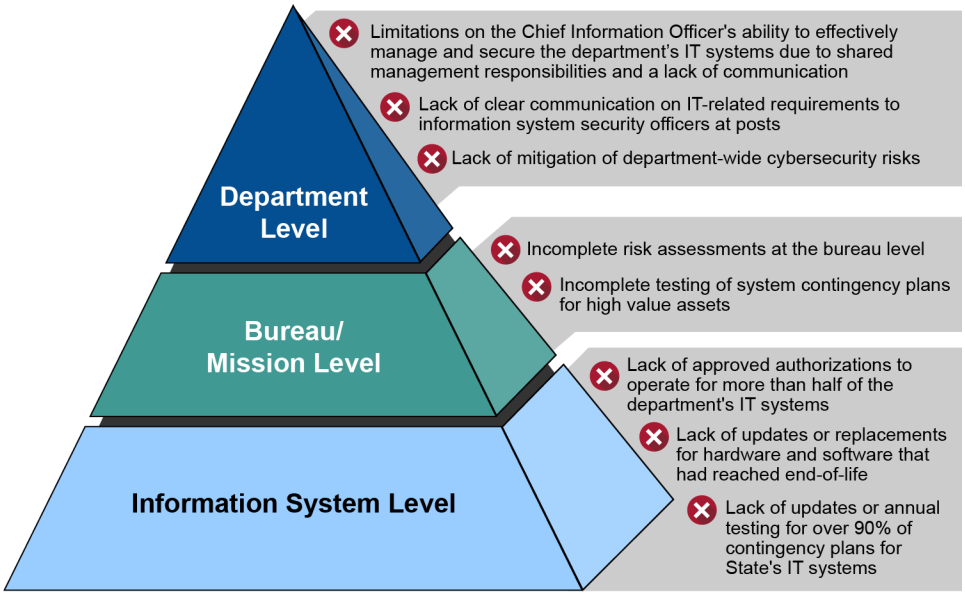
In addition, GAO will issue a subsequent limited distribution report discussing technical security control deficiencies in State's IT infrastructure. The report will identify approximately 40 unique deficiencies across three bureaus and 16 posts and will address about 500 recommendations to State for remediating those deficiencies. These recommendations will include replacing hardware and software installations that have reached end-of-life.

Without fully implemented incident response processes and an adequately secured IT infrastructure to support State's incident response program by, among other things, updating outdated or unsupported products, State's IT infrastructure is vulnerable to exploits. Furthermore, the department risks being unable to fully detect, investigate, and mitigate cybersecurity-related incidents.

In the last several years, State has taken a number of steps to clarify and strengthen the role of the Chief Information Officer (CIO). For example, in October 2020, State issued a memo and matrix outlining the roles and responsibilities for cybersecurity of State's CIO and others.

Nevertheless, the ability of State's CIO to secure the department's IT systems is limited due to shared management responsibilities and a lack of communication. In State's IT structure, the CIO manages State's main network and sets department-wide standards, but bureaus perform many activities independently, purchasing much of their own equipment, managing many of their own IT systems, and obtaining their own funding. In addition, a lack of communication among the CIO, Information Resource Management, and the bureaus also hampers the CIO's ability to secure the department's IT systems. For example, this created confusion among information system security officers about the applicability of IT-related requirements. State's IT structure, insulated culture (i.e., bureaus operating independently), and the lack of communication between the CIO and the bureaus is responsible for many of the deficiencies identified in this report, as shown in the figure below.

Examples of Deficiencies at State Due to Its IT Structure and Insulated Culture



Source: GAO analysis of Department of State documentation. | GAO-23-107012

In October 2021, the CIO noted that the roles and responsibilities matrix needed to be updated to better reflect the specific cyber functions and activities that department leadership and bureaus engage in throughout State. Until State addresses these and other deficiencies, the CIO faces challenges managing and overseeing the department's cybersecurity program, including risk management and incident response, and the department's systems remain vulnerable.