United States Government Accountability Office

Report to Congressional Requesters

September 2023

CYBERSECURITY

State Needs to Expeditiously Implement Risk Management and Other Key Practices

GAO-23-107012

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.

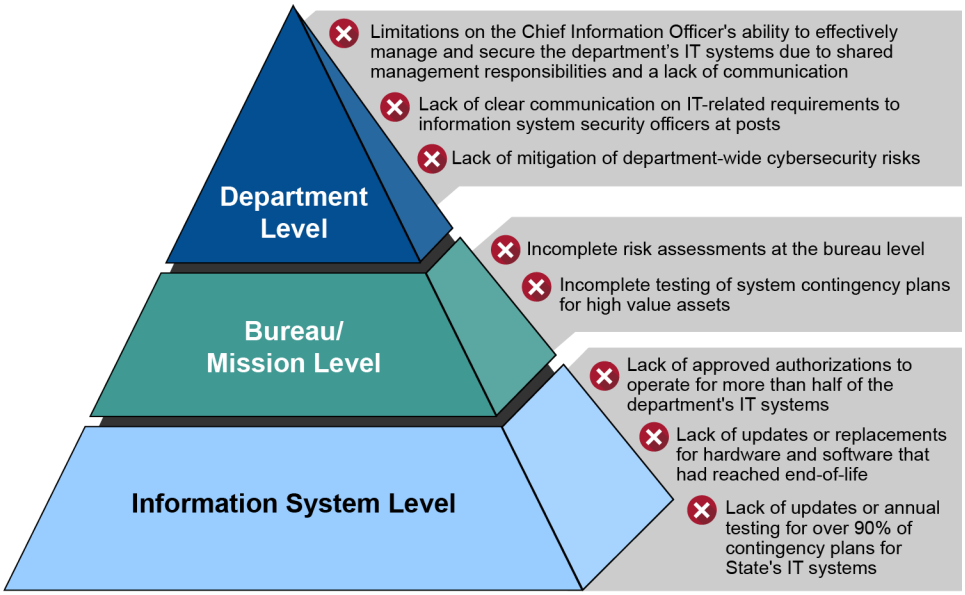
In addition, GAO will issue a subsequent limited distribution report discussing technical security control deficiencies in State's IT infrastructure. The report will identify approximately 40 unique deficiencies across three bureaus and 16 posts and will address about 500 recommendations to State for 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.

Contents

Tables

Figures

Abbreviations

A&A	assessment and authorization
ATO	authorization to operate
CIO	Chief Information Officer
CIRT	cyber incident response team
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	coronavirus disease 2019
DHS	Department of Homeland Security
DS	Bureau of Diplomatic Security
E-CISO	Enterprise Chief Information Security Officer
EOL	end-of-life
FAH	*Foreign Affairs Handbook*
FAM	*Foreign Affairs Manual*
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
GITR	Office of Global Information Technology Risk
HVA	high value asset
IRM	Bureau of Information Resource Management
ISCM	information security continuous monitoring
ISSO	information system security officer
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget
RMF	risk management framework
US-CERT	U.S. Computer Emergency Readiness Team

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

September 28, 2023

The Honorable James E. Risch
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Robert Menendez
United States Senate

The Department of State plays a key role in conducting American diplomacy, helping shape U.S. foreign policy, and supporting U.S. businesses overseas. In addition, State provides and coordinates military, law enforcement, and other assistance to allies. State also provides consular and other services to U.S. citizens, U.S. legal residents, and citizens of other countries. The department conducts this work through its network of domestic offices as well as embassies and consulates overseas.[1]

In performing its mission, State depends on IT systems and the electronic data they store. The security of these systems and the networks to which they connect is crucial to the department's role in promoting an open, interoperable, and reliable information and communications infrastructure. This infrastructure is key to supporting international trade and commerce, strengthening international security, and providing consular services.

Our prior work has shown that it is increasingly important that the department effectively implement cybersecurity practices for securing its systems and networks, including managing its cybersecurity risks.[2] In addition, State's Office of the Inspector General (OIG) has identified a

[1]An embassy, typically headed by an ambassador, is established and maintained by the U.S. government to conduct normal continuing diplomatic relations between the United States and the government of that country. Consulates General operate from facilities located in major cities and represent the offices and staff of consuls general, who are the senior consular representatives of the U.S. government at their overseas posts.

[2]See, for example, GAO, *Information Security: State Has Taken Steps to Implement a Continuous* Monitoring *Application, but Key Challenges Remain,* GAO-11-149 (Washington, D.C.: July 8, 2011).

number of deficiencies in the department's approach to information security, including the lack of an effective information security program.[3]

You requested that we assess State's cybersecurity practices, including the Chief Information Officer's ability to establish and carry out the roles and responsibilities for protecting the department's systems and networks. This report assesses the extent to which (1) State has implemented a cybersecurity risk management program; (2) State has a process and supporting infrastructure (IT assets and personnel with the necessary skills) 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.[4]

This report is a public version of a sensitive report that we issued in August 2023.[5] State deemed some of the information in our August report to be sensitive, which we cannot disclose publicly. Therefore, this report omits the identification of post locations, certain system names, specific technologies, and a specific weakness from all three of our objectives. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

We focused our audit work on the two bureaus that have the main responsibility for managing, overseeing, and securing the department's IT systems and networks: the Bureau of Information Resource Management (IRM) and the Bureau of Diplomatic Security (DS). We also met with high-level officials at the Bureau of Consular Affairs, given that it operates more IT systems than any other bureau.[6] In addition, we met with officials

[3]See, for example, Department of State, Office of Inspector General, *Audit of the Department of State Fiscal Year 2021 Information Security Program,* AUD-IT-22-06 (Arlington, VA: Oct. 2021) and *Audit of the Department of State Information Security Program,* AUD-IT-20-04 (Arlington, VA: Oct. 2019). Note: These reports are not publicly available due to their sensitive nature.

[4]Recently we addressed IT workforce challenges at State. See GAO, *State Department: Additional Actions Needed to Address IT Workforce Challenges,* GAO-22-105932 (Washington, D.C.: July 12, 2022). We found, among other things, that since 2017, State faced IT workforce challenges such as staff concerns regarding low pay and limited incentives and promotions.

[5]GAO, *Cybersecurity: State Needs to Implement Risk Management and Other Key Practices*, GAO-23-103834SU (Washington, D.C.: August 14, 2023).

[6]The Bureau of Consular Affairs provides passport and other services that protect U.S. citizens and their interests abroad. It also issues visas for travelers and immigrants to the United States.

from the Bureau of the Comptroller and Global Financial Services due to that bureau's importance in providing a financial platform to support State's global foreign affairs mission.

For our first objective, we reviewed federal laws, executive orders, Office of Management and Budget (OMB) guidance, and guidance from the National Institute of Standards and Technology (NIST) related to cybersecurity risk management and compared them to department policies. We also compared risk assessments for IT systems and seven system security plans against federal guidance.

To supplement our analysis, we interviewed State officials responsible for managing risk to obtain their perspectives on the department's implementation of the NIST risk management framework (RMF).[7] We also interviewed these officials about whether they experienced challenges in complying with this framework as well as with State's *Cyber Risk Management Strategy*.[8] We interviewed senior IRM officials, including the department's CIO, as well as officials from the IRM's Office of Global Information Technology Risk (GITR) to determine how that office is fulfilling its cybersecurity roles and responsibilities.

For our second objective, we analyzed State's cyber-related policies, procedures, and practices to determine whether the department had a process in place to detect, respond to, and recover from cybersecurity incidents. We also reviewed State's policies and procedures to determine if they aligned with applicable State and NIST guidance. In addition, we selected a nongeneralizable sample of seven systems for review. We selected the department's main sensitive-but-unclassified network,[9] OpenNet, due to the email breach that occurred in 2018.[10] Additionally, we selected six systems that reside on OpenNet, because they have centralized capabilities for State to detect, respond to, and recover from

[7]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, revision 2 (Gaithersburg, MD: Dec. 2018).

[8]Department of State, *Cyber Risk Management Strategy*, version 3.0 (Washington, D.C.: Aug. 2020). Note: This is an internal State document not available to the public.

[9]State defines "sensitive but unclassified" as pertaining to information that is not classified for national security reasons but that requires administrative control and protection from public or other unauthorized disclosure for other reasons.

[10]State suffered a data breach that exposed employee data; the breach affected the department's unclassified email system in 2018, which is part of the OpenNet environment.

cybersecurity incidents. For the same reason, we examined State's contingency plans for the selected OpenNet systems to determine whether the department had developed, updated, and tested them according to NIST guidance. We did not conduct a review of State's classified IT systems.

As part of our review of State's department-wide process of responding to and recovering from cybersecurity incidents, we reviewed State's incident response procedures. We analyzed whether these procedures were documented according to department guidance. We also reviewed a nongeneralizable sample of 25 of State's incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT). We took our sample from a list of incidents reported to US-CERT in fiscal years 2019 through 2021. We selected this sample based on a number of criteria, such as whether classified spillage had occurred and whether the cases were verified.

To determine whether State had a process and supporting infrastructure (IT assets and skills) in place to detect, respond to, and recover from cybersecurity incidents at posts, we reviewed local network switch configuration settings at 16 posts.[11] We used this information to determine if the posts complied with State's switch configuration standards and NIST guidance. We selected our sample based on a variety of criteria such as

- the size of the post,
- the threat potential to the location,
- whether the post had dedicated information system security personnel on-site or was a regional information management center, and
- whether the post was a major hub for activities (including IT activities) conducted by State and other agencies.

For our third objective, we assessed the CIO's ability to secure State's IT systems and factors that might limit the CIO's implementation of cybersecurity practices at the department. Our review included applicable NIST guidance as well as State guidance and documentation describing the roles and responsibilities of IRM, DS, and other bureaus. We compared State's policies and procedures against relevant criteria, such

[11]The term "post" is used to define the various types of diplomatic and consular locations. These include embassies, consulates general, and consulates.

as applicable laws and guidelines, to identify and evaluate the CIO's cybersecurity roles and responsibilities.[12] In addition, we interviewed relevant officials at State to understand how the department's IT infrastructure has changed since the 2018 breach as well as whether the CIO's roles and responsibilities have changed.[13]

As part of our work of determining how State enables the CIO to secure the department's IT systems, we selected a nongeneralizable sample of six posts (both domestic and foreign), for virtual site visits and interviews. We selected the sample based on the same criteria used to determine whether State had a process and supporting infrastructure (IT assets and skills) in place to detect, respond to, and recover from cybersecurity incidents at posts. These interviews addressed, among other things, how IT security procedures are communicated and implemented at posts.

To assess the reliability of data obtained from State (including IT funding data, IT inventory and system information, and information security incident response data), we reviewed documentation and interviewed knowledgeable State officials to corroborate the information in the data. These officials were from the Bureaus of IRM, DS, Comptroller and Global Financial Services, Consular Affairs, and selected domestic and overseas posts.[14] We found that the data we examined were sufficiently reliable for the purposes of our work, except for deficiencies noted in this report. Additional details on our objectives, scope, and methodology can be found in appendix I.

[12]We did not do a full review to determine the extent to which State's funding policies and procedures adhere to the requirements in the law commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA), which consists of provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (2014).

[13]GAO is defining IT infrastructure as encompassing State's IT hardware and software assets (specifically, State's network and system hardware and operating system software). For this IT infrastructure review, GAO evaluated three IT security controls that directly support cybersecurity incident response: IT asset inventory, IT hardware and operating system updates, and audit log coverage and storage.

[14]Among other things, the Bureau of the Comptroller and Global Financial Services is responsible for overseeing all financial activities relating to State's programs and operations.

We conducted this performance audit from October 2019 to August 2023 in accordance with generally accepted government auditing standards.[15] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We subsequently worked with State from August 2023 to September 2023 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Background

State's international mission and business operations require IT systems that are available 24 hours a day, 7 days a week. As of June 2021, State had reported 452 sensitive-but-unclassified IT systems that support its global mission, such as IT systems to process and issue passports and visas. To operate and maintain these systems, State reported spending approximately $11.2 billion in appropriated funds and fees on IT hardware, software, and services in fiscal years 2019 through 2022, including about $1.7 billion on cybersecurity.[16]

State's Organizational Structure and Guidance

State has an intricate organizational structure led by the Secretary of State. The Secretary is assisted by two Deputy Secretaries of State and six Under Secretaries.[17] These Under Secretaries lead six "families" of bureaus and manage 37 bureaus and offices.[18] In addition, State manages numerous offices (e.g., passport offices) throughout the U.S. and more than 270 embassies, consulates, and other posts in almost 200 countries as illustrated in the figure below.

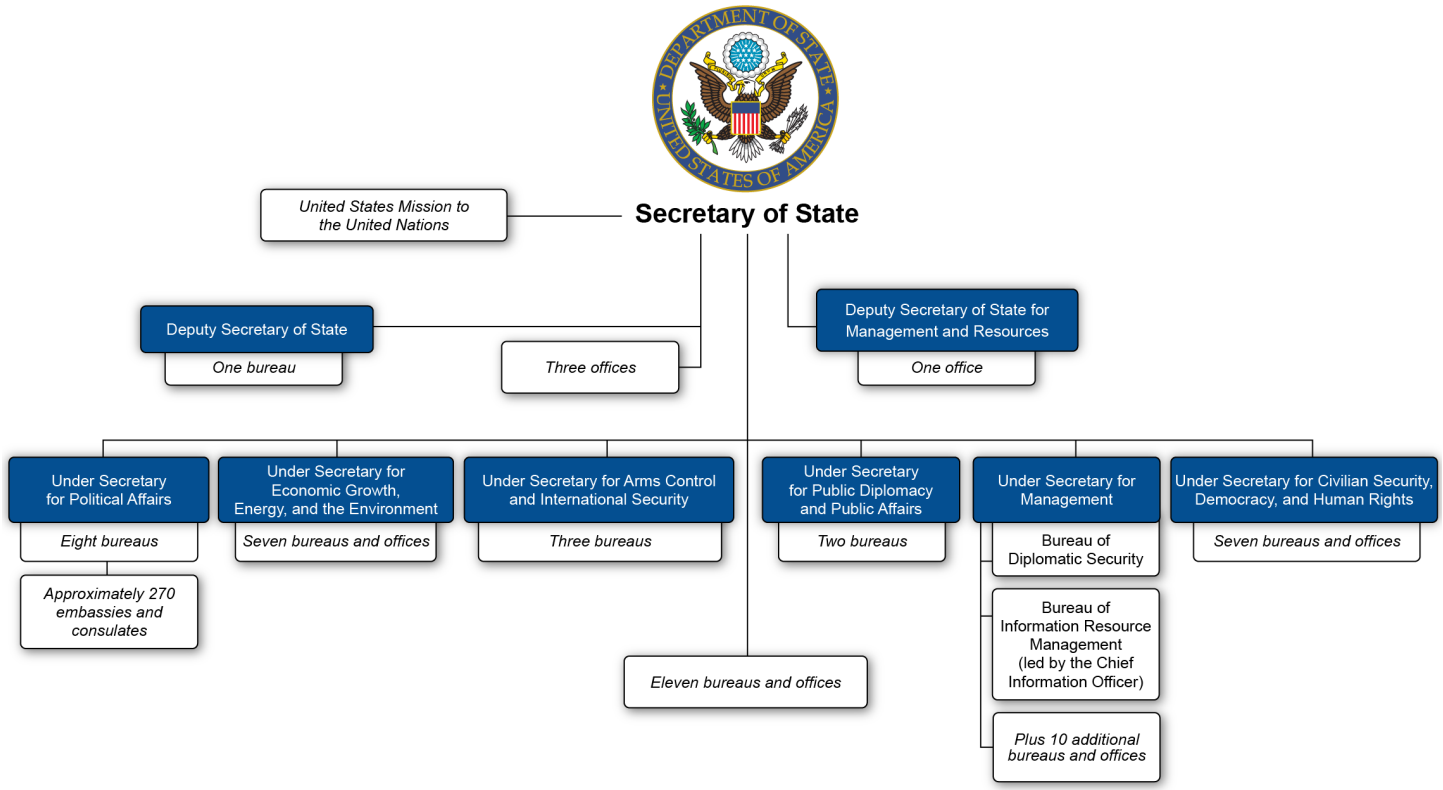
[15]During 2020 and 2021, we made extensive adjustments to the schedule for this work due to the COVID-19 pandemic.

[16]Appendix II provides additional details on State's IT funding in fiscal years 2019 through 2022.

[17]The Deputy Secretary for Management and Resources serves as the principal advisor to the Secretary on the allocation of the department's resources, with assistance from the Under Secretary for Management, the Bureau of Budget and Planning, and the Office of Foreign Assistance.

[18]An additional number of bureaus and offices report directly to the Secretary, the Deputy Secretary, or the Deputy Secretary for Management and Resources rather than to an Under Secretary.

Figure 1: Simplified Depiction of State's Organizational Structure



Sources: GAO (analysis of Department of State documentation); State (logo). | GAO-23-107012

IRM and DS, which have primary responsibility for managing and overseeing the security of State's IT infrastructure,[19] reside within the family of bureaus headed by the Under Secretary for Management. The CIO holds the rank of Assistant Secretary and leads IRM, and an Assistant Secretary leads DS.[20]

State's official policies and procedures (collectively known as directives), including those for cybersecurity, are mainly found in its *Foreign Affairs*

[19]Department of State, Secretary of State, *Modification of IRM and DS Cyber Security Roles and Responsibilities* (Washington, D.C.: Sept. 27, 2004). Note: This memorandum is not available to the public due to the sensitive information it contains.

[20]The Bureau of Diplomatic Security is State's law enforcement and security bureau. It plays a major role in securing State's overseas operations. Within Diplomatic Security, the Directorate of Cyber and Technology Security conducts most cyber activities.

Manual (FAM) and associated *Foreign Affairs Handbooks* (FAH).[21] According to State, the FAM (generally policies) and FAH (generally procedures) combined are a single, comprehensive, and authoritative source for operations. Specifically, the FAM and FAH comprise the organizational structures, policies, and procedures that govern the operations of the department and, when applicable, other federal agencies. According to State officials, memorandums can also be used to communicate changes to its policies and procedures until the needed updates to the FAM or FAH are completed. Memorandums are used between updates due to the length of time involved in implementing changes to the FAM and FAH.

State's IT Infrastructure

State has a federated IT infrastructure.[22] The CIO is the authorizing official for two State enterprise networks, which IRM manages.[23] These networks are intended to allow only authorized connections to systems that the department issues or approves:

1. OpenNet: This is the department's enterprise network that processes, transmits, and stores information up to the sensitive-but-unclassified designation. It provides access to standard desktop applications, such as word processing, email, and internet browsing. OpenNet supports the department's custom software solutions and database management systems.

2. ClassNet: This is an internal network for email and processing of information up to and including the secret classification level.[24]

Due to State's federated IT infrastructure, bureaus share many cybersecurity responsibilities, such as operating and managing their own

[21]Department of State, *Foreign Affairs Manual*, https://fam.state.gov/.

[22]In a federated IT infrastructure, IT activities such as the development of standards, common systems, and an overall architecture are centralized, while IT activities involving specialized application development are done directly by the affected business unit.

[23]An authorizing official is a senior management official or executive with the authority to formally authorize the operation of an information system and accept responsibility for operating the system at an acceptable level of risk to department operations, assets, or individuals.

[24]National security information may be classified at one of three levels depending on the extent of damage to national security that could reasonably be expected if the information is disclosed without authorization. "Top secret" applies to information that could cause exceptionally grave damage, "secret" applies to information that could cause serious damage, and "confidential" applies to information that could cause damage to national security.

systems, which connect to OpenNet. For example, the Bureau of Consular Affairs operates and manages systems that consular officers use in making determinations on visas. In addition, individual posts maintain and manage nonenterprise networks (formerly known as "dedicated internet networks" or DINs) for use by the public to access the internet, among other things.[25] However, the CIO has the overall responsibility to manage and oversee the department's cybersecurity program.

Federal Laws and Guidance Establish CIO Responsibilities

Over the past 27 years, various laws and federal guidance have established roles and responsibilities for federal CIOs to improve the government's performance in IT and related information management functions. In addition, NIST issues guidelines to address and support the security and privacy needs of federal government information and information systems that CIOs should ensure their agencies adopt.

Clinger-Cohen Act of 1996. Under this law, agency heads are required to designate CIOs to help the agency head control system development risks, better manage technology spending, and achieve measurable improvements in agency performance.[26]

Federal Information Security Modernization Act of 2014 (FISMA). FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over federal operations and assets.[27] The law delegates to the agency CIO (or comparable official) the authority to ensure compliance with the requirements in FISMA. In addition, the law requires each agency to develop, document, and implement an agency-wide information security program. This program should provide risk-based protections for the information and information

[25]According to State's *Foreign Affairs Manual*, a dedicated internet network provides access to the internet through an internet service provider on a department-owned-and-operated discrete local area network that is not connected to any other department systems. See Department of State, *Foreign Affairs Manual,* "Dedicated Internet Networks (DIN)," 5 FAM 872 (May 1, 2014), https://fam.state.gov/FAM/05FAM/05FAM0870.html.

[26]40 U.S.C. §§ 11312 and 11313; 44 U.S.C. § 3506.

[27]The Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073 (2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers both to the 2014 act and to those provisions of the 2002 act that were either incorporated into the 2014 act or were unchanged and continue in full force and effect.

systems that support agency operations and assets. FISMA and OMB provisions require agencies to comply with NIST guidelines.

Federal Information Technology Acquisition Reform Act (FITARA). The provisions commonly referred to as FITARA[28] were enacted to further strengthen the authority of federal agency CIOs at the 24 agencies subject to the Chief Financial Officers Act of 1990.[29] FITARA requires State and other covered agencies to ensure that their CIOs have a significant role in the decision-making processes for IT budgeting, management, governance, and oversight. The law includes a provision that gives covered agency CIOs the authority to approve the appointment of other CIOs who operate at office, bureau, and other component levels.

Executive Order 13833, Enhancing the Effectiveness of Agency Chief Information Officers. This order is intended to strengthen the role of agency CIOs by emphasizing that CIOs are required to report directly to their agency head.[30] The order pertains to 22 of the 24 agencies in the Chief Financial Officers Act, including State.

NIST Federal Information Processing Standards 199 and 200. NIST Federal Information Processing Standard 199 requires CIOs and agencies to categorize information and information systems based on an impact assessment. Such an assessment should address the impact a loss of a system's confidentiality, integrity, or availability could have on organizational operations, organizational assets, and individuals.[31]

Standard 200 requires agencies to meet minimum security requirements by selecting the appropriate security controls.[32] These controls are

[28]Provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (2014).

[29]31 U.S.C. § 901(b).

[30]The White House, *Enhancing the Effectiveness of Agency Chief Information Officers,* Executive Order 13833 (Washington, D.C.: May 15, 2018).

[31]National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems,* Federal Information Processing Standards (FIPS) Publication 199 (Gaithersburg, MD: Feb. 2004).

[32]National Institute of Standards and Technology, *Minimum Security Requirements for Federal Information and Information Systems*, FIPS Publication 200 (Gaithersburg, MD: Mar. 2006).

described in NIST Special Publication 800-53,[33] which provides a catalog of baseline security and privacy controls for federal information systems.[34] Additionally, this publication provides a process for selecting controls to protect organizational operations and assets.

State's Cybersecurity and Cyber Risk Management Strategies Established Responsibilities for the CIO and Other Entities

In September 2019, State issued a strategy that laid out the department's cybersecurity program priorities for fiscal years 2019 through 2022.[35] State's cybersecurity strategy focused, in part, on establishing the foundational controls needed to address deficiencies that State's OIG previously identified in the department's information security program. The 2019 strategy moved State from a reactive cybersecurity posture to a more responsive one by emphasizing the need for a stronger IT governance and oversight process.[36] For example, the strategy noted that IRM would need to develop the capacity to monitor IT security from a department-wide perspective rather than by bureau or location.

The strategy also discussed strategic program initiatives for cybersecurity priorities to address State's lack of an effective information security program. For example, one priority program initiative involved the development of an effective asset and inventory management program that was to accurately manage and track hardware and software assets throughout their entire life cycles.

[33]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, revision 5 (Gaithersburg, MD: Sep. 2020). For this audit we evaluated State based on *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, MD: Apr. 2013) since agencies had the option to adopt use of revision 5 right away—once it was finalized in September 2020—or continue to use revision 4 until it was withdrawn on September 23, 2021. Thus, for the majority of our audit, State was still using Special Publication 800-53 revision 4.

[34]Security control topics, referred to as families of security controls, include access control, awareness and training, audit and accountability, assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

[35]Department of State, Office of the Chief Information Security Officer, *Department of State Cybersecurity Strategy, FY 2019–FY 2022* (Washington, D.C.: Sept. 17, 2019).

[36]See for example, Department of State, Office of Inspector General, *Management Assistance Report: Deficiencies Reported in Cyber Security Assessment Reports Remain Uncorrected*, ISP-17-39-01 (Arlington, VA: July 2017).

In addition to the cybersecurity strategy, in August 2020, State developed a *Cyber Risk Management Strategy*.[37] The strategy communicated the parameters for identifying, assessing, responding to, and monitoring risks associated with the operation of information systems owned and contracted by State. The strategy also identified roles and responsibilities for the CIO, the heads of bureaus, and others associated with ensuring the cybersecurity of the department's IT systems.[38] Table 1 describes these roles and responsibilities.

Table 1: Principal Officials with Roles and Responsibilities for Cybersecurity at State

Role	Responsibility
Chief Information Officer (CIO)	Is to ensure the availability of State's IT systems and operations to support the department's diplomatic, consular, and management operations. The CIO is to serve as the designated accrediting authority for all IT systems department-wide up to the secret level.[a]
Enterprise Chief Information Security Officer (E-CISO)	Is to serve as the accountable senior executive for the department's cybersecurity program. The E-CISO is responsible for directing and reporting department-wide compliance with current and emergent federal and legislative cybersecurity mandates to departmental leadership, the Office of Management and Budget, and Congress.
The Bureau of Diplomatic Security's Deputy Assistant Secretary and Assistant Director for Cyber and Technology Security	Is responsible for operating a Joint Security Operations Center in conjunction with the Bureau of Information Resource Management to detect cyber threats. This individual is to provide situational awareness through analyses of cyber threats, technical vulnerabilities and network activity to protect against cyber adversaries. This individual is also responsible for directly managing State's Cyber Incident Response Team.
System owner	Is responsible for operating specialized software and hardware. Within the bureaus, bureau-authorizing officials are designated as the primary IT system owners at the department, but some system owners are located at offices and posts.
Information management officer / information systems officer / system administrator	Is to develop and maintain system security plans for all IT systems and major applications for which the officer or administrator is responsible. This individual is also to participate in risk assessments to periodically re-evaluate the sensitivity of system, risk, and mitigation strategies.
Information system security officer (ISSO)	Is to ensure systems are configured, operated, maintained, and disposed of in accordance with all relevant State security guidelines. The ISSO is the formally designated official responsible for enforcing information system security policies at the department. The responsibilities for this position are typically assigned to an information management officer as a collateral duty.

[37]Department of State, *Cyber Risk Management Strategy*, version 3.0.

[38]These roles and responsibilities were modified in an October 2020 memo. See Department of State, Under Secretary for Management, *Department Cybersecurity Roles and Responsibilities 2020 and Beyond,* memorandum (Washington, D.C.: Oct. 22, 2020). Note: This memorandum is not available to the public due to the sensitive information it contains.

Role	Responsibility
Regional cybersecurity officer	Is to perform periodic cybersecurity assessments of State systems at posts to determine compliance with regulations as well as improvements needed. A regional cybersecurity officer can also assist ISSOs as needed and must report to the Bureau of Diplomatic Security.

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

[a]A designated accrediting authority or authorizing official is a senior management official or executive with the authority to formally authorize the operation of an information system and accept responsibility for operating the system at an acceptable level of risk to department operations, assets, or individuals. State's Bureau of Intelligence and Research serves as the accrediting authority for all State IT systems classified above the secret level.

State Documented a Program for Cybersecurity Risk Management but Has Not Fully Implemented It

State documented a program for cybersecurity risk management that aligns with the NIST Risk Management Framework (RMF). For example, the program includes the identification, implementation, and documentation of cybersecurity roles and responsibilities as well as strategies for cybersecurity risk management and continuous monitoring.

However, the department has not fully implemented its risk management program at the department, bureau, and system levels to identify and monitor risk to assets and the information maintained on its systems.[39] For example, State has not

- fully assessed its department-wide cybersecurity risks nor developed plans to mitigate vulnerabilities,
- completed bureau-level cybersecurity risk assessments,
- completed system-level risk assessments for its high value assets,
- consistently reviewed and updated system security plans,
- fully assessed and authorized its information systems for operation,
- fully documented requirements in its continuous monitoring strategy for information security, nor
- implemented a department-wide continuous monitoring program at bureaus and posts.

[39]Following the National Institute of Standards and Technology's *Risk Management Framework for Information Systems and Organizations* (RMF), the department's program for cybersecurity risk management assigned tier 1 strategic risks at the department level, tier 2 risks at the bureau or mission level, and tier 3 risks at the systems level.

For this objective, we have omitted sensitive information that is contained in our August 2023 report.[40] The omitted information includes the identification of certain system names and specific technologies.

State Documented a Program for Cybersecurity Risk Management That Is Consistent with Federal Guidance

The NIST RMF emphasizes the importance of documenting a holistic approach to risk management that must take place at the department, bureau, and information system levels.[41]

The NIST RMF "prepare" step describes the five actions federal departments and agencies should take to establish a risk management program at the organizational level (see table 2). The purpose of this step is to carry out essential activities at the organization (or department), mission (or bureau), and information system levels of the organization to help prepare the organization to manage its security risks using the RMF.

Table 2: Activities Included in the NIST Risk Management Framework Prepare Step at the Organizational Level

"Prepare" activity	Activity description
1. Assign security and privacy risk management roles and responsibilities	Organizations should identify and assign individuals to specific roles associated with security and privacy risk management. In coordination with senior leaders and executives, organizations should establish the risk executive function. This function is to serve as the common risk management resource for groups, offices, and personnel assigned to cybersecurity roles. It provides a comprehensive, organization-wide approach and guidance to risk management. The risk executive ensures that risk management is consistent throughout the organization, reflects organizational risk tolerance, and considers cybersecurity along with other types of risk to ensure mission and business success.
2. Document a security and privacy risk management strategy	The risk management strategy is to guide and inform risk-based decisions, including how security and privacy risk is framed, assessed, responded to, and monitored. The strategy is to include the threats, assumptions, constraints, priorities, trade-offs, and risk tolerance used for making investment and operational decisions. The strategy is also to include (1) acceptable risk assessment methodologies and risk response strategies; (2) a process for consistently assessing security risks across the organization, its business units (or bureaus), and its information systems; and (3) approaches for monitoring risk over time.
3. Identify common security controls	Common controls are controls that one or more information systems can inherit. Organizations identify and select the set of common controls and allocate them to common control providers. By identifying common controls, organizations can reduce the time and cost to implement security controls, perform assessments, obtain an authorization to operate (ATO), and perform continuous monitoring. In addition, common controls focus organizational resources to harden, expand, and improve the delivery of shared security services rather than spread cost and effort across numerous systems. Organizations may establish one or more lists of common controls that information systems can inherit. A common control may not fully meet a requirement. In such cases, the control is considered a hybrid control and the organization notes it as such. This includes specifying which parts of the control requirement the common control provides for inheritance and which parts are to be provided at the system level.

[40]GAO-23-103834SU.

[41]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, revision 2.

"Prepare" activity	Activity description
4. Assess security and privacy risk at the department, bureau, and system levels	Organizations should develop and document security assessment plans and then assess security and privacy risks at the department, bureau, and system levels to consider the totality of risk from the operation and use of information systems. Any control deficiencies identified during the assessment should be remediated to address the deficiencies in the systems and department-wide environment of operation. Risk decisions made at the department and bureau levels should guide and inform how an agency will address risk from an information system perspective. Organizations should conduct risk assessments of information systems throughout the system's life cycle to support various RMF steps and tasks. Risk assessment results are used to inform processes such as (1) defining security requirements; (2) categorizing risks; (3) selecting, tailoring, and implementing controls; (4) making authorization decisions; (5) determining potential courses of action and priorities for risk responses; and (6) implementing a continuous monitoring strategy for information systems.
5. Implement an organization-wide strategy for continuously monitoring control effectiveness	The organizational continuous monitoring strategy is to address monitoring requirements at the organization, mission (or bureau), and information system levels. The continuous monitoring strategy (1) identifies the minimum frequency for monitoring implemented controls across the organization, (2) defines the ongoing control assessment approach, and (3) describes how ongoing assessments are to be conducted (e.g., addressing the use and management of automated tools and providing instructions for ongoing assessment of controls for which monitoring cannot be automated). Organizational officials, including the risk executive, collaborate to establish the criteria for determining the minimum frequency for control monitoring. An organizational risk assessment can be used to guide and inform the frequency of monitoring.

Source: GAO analysis of National Institute of Standards and Technology (NIST) documentation. | GAO-23-107012

Note: The NIST Risk Management Framework describes risk management activities for both security (which includes cybersecurity risk management) and privacy; however, our review focused on security (i.e., cybersecurity) risk management practices at the Department of State but not privacy. See National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, revision 2 (Gaithersburg, MD: Dec. 2018).

State has documented a program for cybersecurity risk management that meets NIST requirements. Specifically, the department has taken steps to manage its security risks using the NIST RMF as a guide. To this end, State issued various relevant policies and procedures in its FAM, FAH, and RMF playbook. State also issued a risk management strategic plan that included specific roles and responsibilities as well as the policies and procedures the department is to follow for its risk management program.[42]

Activity 1: State Identified Risk Management Roles and Responsibilities

In its FAM, FAH, and other organizational charters, State assigned various individuals and entities within its bureaus specific roles and responsibilities to carry out cybersecurity-related activities, including

[42]Department of State, *CyberOperations RMF Playbook Workflow 1.4* (Washington, D.C.: Apr. 15, 2021). Note: This is an internal State document not available to the public. The playbook provides referential guidance on how to manage the assessment and authorization process for information systems.

those specific to risk management. Table 3 describes these entities and their risk management–specific roles.

Table 3: Summary of Key Risk Management Roles for Overseeing and Managing Cybersecurity Risk at State

Entity	Description of role
Bureau of Information Resource Management (IRM)	IRM is to facilitate system risk assessments and authorizations (A&A) for the Chief Information Officer (CIO). The A&A process is to include a comprehensive evaluation of an information system's technical and nontechnical security components, documentation, supplemental safeguards, policies, and vulnerabilities. At the information system level, the CIO acts as the authorizing official with responsibility for accepting risks affecting IT systems. To that end, the CIO is to oversee all decisions related to cyber risk management for the department on behalf of the Secretary, even in cases where bureaus are delegated authority to make risk decisions affecting mission-specific systems.
Office of Global Information Technology Risk (GITR)	GITR, an office within IRM, is responsible for developing department-wide IT risk assessment policies, procedures, and templates to guide State organizations responsible for IT in conducting their own IT risk assessments. State organizations and bureaus responsible for IT (including the department's high value assets) are allowed to conduct their own IT risk assessments and report the results to GITR. GITR is to analyze these reports, identify risk trends, and present their findings to department leadership to increase situational awareness and inform risk management decisions. Additionally, GITR is responsible for issuing bureau-level risk scorecards to communicate cybersecurity risks affecting bureaus. GITR is also to fill the role of the risk executive. This includes providing oversight and consultation to ensure that cybersecurity practices at the department, bureau, and systems levels are implemented in a manner consistent with the department's *Cyber Risk Management Strategy*. In its role as the risk executive, GITR is to serve primarily as a consultant at the bureau and information system levels.
Assessment and Authorization Division	The division's functions include overseeing the implementation of the RMF throughout the department, including developing guidance and providing oversight to bureau system owners by ensuring that department systems are compliant with FISMA. The A&A division's responsibilities include implementing the A&A process, testing contingency plans, and managing common controls. The division established State's A&A workflow procedures and processes to lead to the CIO providing an authorization to operate for the department's information systems and common controls.[a]
Bureau of Diplomatic Security	This bureau is responsible for the department's communications, information, physical infrastructure, and cybersecurity as part of its mission to protect personnel, diplomatic missions, and information. The bureau is to provide the department with cyber threat intelligence, vulnerability analysis, and technical security assessments necessary to support its officials in making informed risk management decisions.
Information system owners	The information system owner at the bureau level is an official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. In terms of cybersecurity, the system owner is responsible for ensuring that the information system is compliant with all applicable National Institute of Standards and Technology and State requirements. System owners are to facilitate the activities related to the A&A process for the information systems they own and to prepare and submit all required A&A-related paperwork. The system owners are then to submit the final A&A paperwork to the CIO for an authorization to operate and continuously monitor the information system for risks, threats, and vulnerabilities to the confidentiality, integrity, and availability of the system's information.

Entity	Description of role
Enterprise Governance Board	The board is a high-level forum for senior State leaders to discuss strategic issues and provide input into enterprise-level decisions. It has decision-making authority and is accountable for providing direction at the strategic level on the integration of risk management practices into business operations and decision-making. The Deputy Secretary of State is to chair the board, and permanent membership is to include all department Under Secretaries. While not a member of the board, the CIO is to advise members on enterprise cyber risks for the board to consider in overall State operations management.
IT Executive Council	The council is an advisory body that is chaired by the CIO and is intended to deliberate IT issues, including cybersecurity and risk management. The council established two working groups: cybersecurity and risk and resiliency. These working groups are to serve as the governing authorities within State to manage technology risks by, for example, making decisions for implementing appropriate mitigating controls on cyber activities that exceed the department's risk tolerance. The council is to populate a department-wide risk profile for submission to the Enterprise Governance Board, and the council's work is intended to inform the board's decisions.
Enterprise Chief Information Security Officer Council	The council is to implement State's cybersecurity strategy through collaboration among bureau chief information security officers and IT security officers to identify cybersecurity solutions, best practices, and strategies. The council is to meet to discuss cybersecurity risks across the department, its bureaus, and its information systems. The council is charged with improving cybersecurity performance with a focus on making recommendations concerning cybersecurity department-wide and providing strategic cybersecurity expertise.

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

[a]The *Foreign Affairs Handbook* defines authorization to operate (ATO) as the requirement for the CIO or other authorizing official accepting the risk of unclassified information systems and application systems in the form of an ATO before commencing operations. The information systems and application systems must undergo reassessment and reauthorization every 3 years or when there is a significant change to the system. Department of State, *Foreign Affairs Handbook*, "System Assessment and Authorization," 12 FAH-10 H-310 (Mar. 8, 2019). Note: This is an internal State document not available to the public.

Activity 2: State Developed a Cyber Risk Management Strategy

In August 2020, State released the third version of its *Cyber Risk Management Strategy*.[43] The strategy is to serve as a guide for department planning, operations, and governance through the incorporation of cybersecurity risk management in accordance with NIST guidance. According to the strategy, organizational direction for cybersecurity is established at the department level. This includes establishing priorities for cyber activities based on mission function and cyber risk tolerance.[44]

Bureau-level authorizing officials are expected to make decisions within the scope of the department's established risk tolerance.[45] This includes the responsibility of managing the risk of bureau systems operating at the information system level. At this level, system owners and staff are expected to maintain the daily operations and functions of department information systems and assets within the prescribed ranges of risk tolerance.

The 2020 strategy includes an expression of organizational risk tolerance, acceptable risk assessment methodologies and risk response strategies, and approaches for monitoring risk over time. The strategy also includes risk categories that align with NIST guidance, ranging from very low (risks that could have a negligible adverse effect on the organization) to very high (risks that could have a catastrophic effect on the organization).

The strategy calls for the department to perform risk assessments at the department, bureau, and information system levels. At the department level, risk assessments focus more on information security program efforts and significant system vulnerabilities. At the bureau level, bureaus are to consider the impact of identified system-level weaknesses to their operations. System-level risk assessments are to identify system-specific vulnerabilities and the degree of exposure to the system. The department is to conduct these assessments in accordance with NIST guidance. In

[43]Department of State, *Cyber Risk Management Strategy,* version 3.0.

[44]As stated in the strategy, risk tolerance is the acceptable level of variance from the risk appetite that is considered acceptable relative to the achievement of the mission and its objectives. Risk appetite is the broad-based amount of risk an organization plans to accept in pursuit of its mission and vision. It is established by the organization's most senior level leadership and serves as a guidepost to set strategy and select objectives.

[45]Bureau-level authorizing officials can be mission owners who are aligned to bureaus and who have statutory, management, or operational authority and responsibility for specified information. Mission owners apply State's policies and establish procedures for governing the generation, collection, processing, dissemination, and disposal of the specified information they own.

addition, OMB requires[46] federal departments and agencies to conduct risk assessments of their high value assets (HVA) at a scheduled frequency determined by the Department of Homeland Security (DHS).[47]

Activity 3: State Documented Procedures for Identifying Common Information System Controls

State's RMF playbook documents procedures for identifying common information system controls. State's assessment and authorization (A&A) division is responsible for department-wide common control management. According to NIST, a common control is a security control inherited by multiple information systems or programs. The department's RMF playbook requires information system owners to select and document security controls in a system security plan that include tailoring common controls supplied by the department's common control providers to suit the security needs of the systems.[48]

Activity 4: State Documented Processes to Assess Cybersecurity Risk in Information Systems

State documented processes to assess cybersecurity risk. For example, to supplement the risk management process outlined in the *Cyber Risk Management Strategy*, State issued the RMF playbook.[49] The playbook describes State's adoption of the NIST RMF, including detailed steps for conducting the A&A process for information systems.

According to the playbook, information systems at the department are required to go through the A&A process prior to moving into production and must maintain authorized status (or authorization to operate) to continue operating. Information systems that have not undergone this process are required to do so.

The playbook further states that the department should disconnect from its network any information systems that do not receive or maintain an authorization to operate (ATO) until one is granted. This minimizes risk to the department, to bureaus, and to State's information systems. The

[46]Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018).

[47]A high value asset (HVA) is a designation for federal information or a federal information system that is considered vital to an agency fulfilling its primary mission or is considered essential to an agency's security and resilience. See GAO, *Priority Open Recommendations: Department of Homeland Security*, GAO-22-105702 (Washington, D.C.: July 15, 2022).

[48]Examples of available common controls at the department include assessment and authorization, plan of action and milestones management, penetration testing, incident response, and vulnerability scanning.

[49]Department of State, *CyberOperations RMF Playbook Workflow 1.4*.

playbook also includes a variety of reasons an information system may need to be reauthorized, including the potential impact these types of changes may have on the system's security, such as

- the addition and removal of software features,
- the implementation of significant software patches (upgrading or downgrading operating systems, database management systems, and the application),
- configuration changes, and
- open plan of action and milestone items.

The playbook describes the activities State should perform for each step of its RMF, in accordance with NIST guidance. Table 4 describes each step of State's RMF playbook through system authorization, and a summary of the activities that are to be completed for each step.

Table 4: State Risk Management Framework (RMF) Playbook Steps through Authorization and a Summary of Key Activities for Each Step

RMF step	Step description	Summary of key activities
Categorize	The information system owner is to identify the types of information being processed, transmitted, and stored by the information system and then use National Institute of Standards and Technology (NIST) guidance to place those information types into predefined categories.[a] This step is also intended to allow State to build an in-depth inventory of systems and equipment.[b]	• Categorize the information. • Determine the level of risk and the level of protection required for the categorized information using federal guidance based on confidentiality, integrity, and availability. • Determine the overall risk level (based on the highest level of risk).
Select	The information system owner is to select baseline controls (minimum required security controls) and inherited or common controls (controls developed, managed, and implemented by entities other than those responsible for the information system).	• Select baseline and common or inherited controls from NIST guidance.[a] • Determine how frequently the controls should be reassessed.
Implement	The information system owner is to document the implementation of the controls selected during step 2 ("Select"). Implementation refers to the actions taken to ensure that the security controls have been satisfied. This can be accomplished through various means, including a code fix, a patch, or the creation and distribution of a policy and procedure.	• Divide implemented controls into security control families based on NIST guidance.[a] • Provide a technical explanation of how each control is to be implemented. • Determine whether each control is planned to be implemented, has been implemented, or has a compensating control. • Document the controls and their implementation status in a system security plan. • Develop a plan to test the selected technical NIST controls and document it in the security assessment plan.[a]

RMF step	Step description	Summary of key activities
Assess	A security controls assessor, a third party not directly affiliated with the information system, is to evaluate the security controls that have been selected for the assessment.	• Conduct the controls testing in accordance with the security assessment plan. • Document the findings of the test in a security assessment report. • For any controls that were not fully implemented or remediated within 15 days of the assessment, the authorizing official's designated representative should reach out to the information system owner before developing a plan of action and milestones to document the remediation steps for the control. The plan of action and milestones should detail resources required to accomplish elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. • Review and update the system security plan annually or as major modifications occur as required by the *Foreign Affairs Handbook*.[c]
Authorize	The department's authorizing official, the Chief Information Officer (CIO), is to grant or deny a system owner's request for an authorization to operate for an information system. The CIO is to weigh the results of the risk assessment and the recommendations of other reviewers to determine under what conditions an authorization should be granted and for how long. Additionally, the CIO is to determine if the information system presents too great a risk and is not yet ready for operation.	• The CIO or a designee considers the overall risk impact and the current and historical status of the information system (what level of risk it has posed in the previous months and years, what historical security issues remain outstanding, etc.). • The CIO or a designee reviews the artifacts from the previous RMF steps, including the security assessment report. • The CIO provides an authorization to operate or denies authorization. The authorization to operate includes an acceptance of the unmitigated risks identified in the risk assessment results.

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

[a]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, MD: Apr. 2013) (withdrawn as of Sep. 23, 2021).

[b]Department of State, *CyberOperations RMF Playbook Workflow 1.4* (Washington, D.C.: Apr. 15, 2021). Note: This is an internal State document not available to the public.

[c]Department of State, *Foreign Affairs Handbook*, "System Security Plan," 12 FAH-10 H-322.1 (Oct. 15, 2018). Note: This is an internal State document not available to the public.

Activity 5: State Documented a Continuous Monitoring Strategy

In October 2020, the department issued its *Department of State Information Security Continuous Monitoring Strategy*.[50] The strategy applies to all departmental entities operating information systems or collecting and maintaining information. The strategy is to be implemented after the systems undergo the initial security authorization previously

[50]Department of State, *Department of State Information Security Continuous Monitoring Strategy*, version 1.4 (Washington, D.C.: Oct. 9, 2020). Note: this is an internal State document not available to the public.

described and throughout the operation of the system until it is decommissioned.

According to the strategy, the objectives of the department's continuous monitoring efforts include

- communicating defined risk tolerance levels to support risk management,
- defining metrics to provide meaningful indications of the information systems' security,
- assessing security controls to ensure continued effectiveness of their implementation and operation, and
- establishing and maintaining an accurate asset inventory, including all systems, devices, and software across the department.

According to the strategy, each information system owner is to develop and maintain a plan for continuous monitoring of system controls to maintain an understanding of cybersecurity control effectiveness and status. The plan should include how the security controls are monitored for effectiveness and how frequently the controls should be assessed.

The strategy identifies various ways the department intends to continuously monitor the security posture of its information systems and a general approach for doing so, including the following:

- *Configuration management*. Controlling IT system components, features, and assurances defined as configuration items by monitoring changes to a system's hardware, software, firmware, testing, and test fixtures throughout the life cycle of a system.
- *Configuration monitoring*. Monitoring the system to ensure all components are configured in accordance with department configuration requirements.
- *Vulnerability monitoring*. Maintaining an understanding of the vulnerabilities and remediations that have been identified for software and hardware the department has deployed.
- *Automated security control assessments*. Establishing a continuous diagnostics and mitigation program developed by the Department of Homeland Security that provides automated tools to assess controls

on a frequent basis (as defined by DHS)[51] and aggregate and feed results into a dashboard for review, prioritization, and remediation of identified weaknesses.

We have previously reported on State's efforts to develop and document policies for managing cybersecurity risk.[52] In that report, we made two recommendations, which remain unimplemented, for State to

- update the department's policies to require (1) an organization-wide risk assessment, (2) an organization-wide strategy for monitoring control effectiveness, (3) system-level risk assessments, (4) the use of risk assessments to inform security control tailoring, and (5) the use of risk assessments to inform plan of action and milestone prioritization; and
- establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

For the first unimplemented recommendation, State has updated several of its cybersecurity policies, but as of June 2023, it had not yet provided evidence that these policies fully addressed the elements identified in our recommendation.

For the second unimplemented recommendation, State has not yet provided us with sufficient documentation of its actions to fully establish a process for coordinating between its cybersecurity risk management and enterprise risk management functions.

[51]The White House, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements, M-21-02* (Washington, D.C.: Nov. 9, 2020). The goal of the continuous diagnostics and mitigation program is to enhance the overall security posture of the federal government by providing federal agencies with capabilities to monitor vulnerabilities and threats to their networks in near real time. This increased situational awareness is intended to allow agencies to prioritize actions to mitigate or accept cybersecurity risks based on an understanding of the potential impacts to their mission. Continuous diagnostics and mitigation works with agencies to deploy commercial off-the-shelf tools on agency networks that provide enterprise-wide visibility of what assets, users, and activities are on their networks. This actionable information can then enable agencies to effectively monitor, defend, and rapidly respond to cyber incidents.

[52]GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019).

State Has Not Fully Implemented Its Program for Cybersecurity Risk Management

Although State has established a program for cybersecurity risk management by documenting activities two through four prescribed in the NIST RMF prepare step, it has not fully implemented them.[53] Specifically, the department has not mitigated identified risks and has not always performed risk assessments at the department and bureau levels. Though State has plans for system-level risk assessments of its HVAs, it has not yet completed most of these assessments. Furthermore, the department did not authorize all information systems, review and update system security plans for key systems with the required frequency, or implement key capabilities for continuous monitoring.

State Has Not Fully Assessed Department-Wide Cybersecurity Risks nor Developed Mitigation Plans

OMB requires that federal agencies develop and maintain a risk profile that prioritizes the most significant risks identified during the risk assessment process.[54] In addition, the NIST RMF states that any control deficiencies identified during the risk assessment should be mitigated to address the deficiencies in the department-wide environment of operation.[55]

In completing the first phase of its assessment in June 2021, State identified areas of exposure and threats to its department-wide IT environment and vulnerabilities for each area of exposure.

Although State completed the first phase of its risk assessment, it has not established a department-wide risk profile, which is intended to be a prioritized inventory of the most significant risks identified and assessed through the risk assessment process. In addition, State has not developed plans to mitigate the vulnerabilities that it identified in its department-wide risk assessment. Department officials stated that State planned to conduct another department-wide cyber risk assessment by December 2022 and establish a risk profile and baseline. However, State has not provided evidence of having completed these activities.

Officials stated that the department has developed a cybersecurity framework dashboard to establish a risk profile and baseline. This

[53]Activity 1 is discussed further in the section of the report on CIO oversight as it relates to the risk executive and how risks are managed throughout the organization.

[54]Office of Management and Budget (OMB), *OMB Circular No. A-123 Management's Responsibility for Enterprise Risk Management and Internal Control,* M-16-17 (Washington, D.C.: July 15, 2016).

[55]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, revision 2.

dashboard is intended to enable the department to appropriately mitigate and respond to areas of exposure and threats to its department-wide IT environment. However, State did not provide us with evidence that it had implemented this dashboard.

Identifying department-wide cybersecurity risks as well as areas of exposure and threats and associated vulnerabilities can position State to mitigate these areas. Without doing so, State is at increased risk that malicious actors will compromise its information systems.

State Has Not Always Assessed Bureau-Level Cybersecurity Risks

Although the NIST RMF requires risk assessments at the department, bureau, and system levels of the organization, State has not completed the majority of the required bureau-level risk assessments. Specifically, the department assessed cybersecurity risks from systems supporting three of its 31 bureaus that owned information systems—Consular Affairs; Population, Refugees, and Migration; and Political-Military Affairs.

State officials in the Office of Global Information Technology Risk (GITR) stated that the department does not always perform bureau-level risk assessments because the bureaus have to balance completing the assessments with working to meet their ongoing high-priority missions. GITR officials added that open communication with bureaus, a shared understanding of the value of assessing risk, and planning bureau-level risk assessments as far in advance as possible could help to provide that balance.

In addition, GITR officials stated that the department has completed two more bureau-level risk assessments and plans to complete an additional 10 bureau-level risk assessments during fiscal year 2023. Further, to facilitate these assessments, GITR officials stated that the department has developed a cybersecurity framework dashboard where bureaus can view their current risk profiles. While State provided sample screenshots of the dashboard showing a generic risk profile, the department has not provided further evidence that it had completed the risk assessments.

Until the department completes all bureau-level risk assessments, State will continue to have gaps in its understanding of the cybersecurity risks to its bureaus. These gaps may hinder its ability to protect information systems that are key to supporting its mission.

State Has Not Assessed System-Level Cybersecurity Risks for Most of Its High Value Assets

OMB requires that DHS's Cybersecurity and Infrastructure Security Agency (CISA)[56] or an executive agency's independent assessors conduct assessments of HVAs.[57] State has not completed system-level risk assessments for most (90 percent) of these assets as required by OMB but has plans to do so.

Specifically, in the summer of 2022, State completed assessments for 10 percent of its HVA systems, which the Consular Affairs and Global Talent Management bureaus own. GITR officials stated that the department has a plan and draft schedule for assessing the remaining assets. Moreover, GITR officials stated that CISA is scheduled to assess 10 percent of its HVAs in fiscal year 2023.[58]

According to GITR officials, the department has not performed assessments for all of its HVAs because it has not found independent assessors to perform the work. GITR officials added that the department plans to complete the remaining assessments by identifying and training internal staff to obtain a CISA assessment evaluation and standardization certification. This certification would qualify staff to conduct HVA assessments not led by CISA. The department plans to complete staff certification in 2023.

State Assessed Cybersecurity Risk for Key Systems but Did Not Consistently Review and Update the Corresponding System Security Plans

Department policies require annual reviews and updates of system security plans to include identification of the applicable security controls and an inventory of components within the boundary of the information system.[59] Of the seven systems we selected for review, State assessed risk and updated the system security plan for one system. However, the department did not provide documentation showing annual reviews and updated system security plans for the other six systems.[60]

[56]Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03.

[57]Department of Homeland Security, *Securing High Value Assets,* BOD 18-02 (Washington, D.C.: May 7, 2018).

[58]Per BOD 18-02, federal departments and agencies are required to submit a prioritized list of their HVAs to DHS and update the list on a quarterly basis. DHS then selects HVAs that they will assess, in coordination with the department or agency, through CISA.

[59]Department of State, *Foreign Affairs Handbook*, "System Security Plan," 12 FAH-10 H-322.1 (Oct. 15, 2018). Note: This is an internal State document not available to the public.

[60]Prior security plan reviews for these systems were two to four years old.

In addition, State had not identified the type of security controls that applied to the systems—common, system-specific, inherited, or hybrid—for three of the seven selected systems.

Lastly, State did not previously document the inventory of all information system components that fall within the authorization boundary of the information system. Specifically, State had not been documenting an inventory of equipment for two systems.

State officials noted that the department was in various stages of updating the system security plans in accordance with State's A&A process. State reviewed and updated system security plans for four of the seven systems we reviewed.

In 2023, we verified that these updates included documenting the type of security controls and inventory for those four systems. However, State has not yet annually reviewed and updated the remaining two system security plans. Until State ensures that it reviews and updates its system security plans annually in accordance with its policies, the department will not have an up-to-date baseline of controls for its mission-critical systems.

State Did Not Complete Assessments of Cybersecurity Risk by Authorizing Systems to Operate

State's RMF playbook requires the CIO to grant or deny requests for authorization to operate (ATO) information systems.[61] However, as of June 2021, State had not received an authorization from the CIO to operate for over half of its information systems. Specifically, State had not authorized the operation of 276 of its 494 information systems (approximately 56 percent) through its A&A process.[62] The unauthorized systems included the following:

- 15 HVA systems
- Seven high-risk systems (including one HVA)

[61]Department of State, *CyberOperations RMF Playbook Workflow 1.4*.

[62]These systems were all critical to State missions and the majority of them were systems State bureaus owned, developed, and operated.

- 119 moderate-risk systems[63]

According to State officials, the following factors contributed to the backlog in authorizing information systems:

- **Resource constraints:** The Bureau of Consular Affairs—the bureau that owns the most IT systems—attributed the authorization backlog to resource constraints related to time, money, personnel, and expertise in the RMF process. For example, bureau officials stated that resolving vulnerabilities identified during the risk assessments is a resource-intensive process. According to these officials, unless the number of high and moderate vulnerabilities is mitigated to an acceptable level of risk, the CIO will not grant a full authorization to operate to a system. Bureau officials added that they have been in frequent communication with IRM to resolve the system authorization backlog for their systems.
- **COVID-19 constraints:** A Bureau of Consular Affairs official stated that prior to the pandemic, the bureau had a hiring freeze that affected its ability to fill vacant positions. In addition, effects of the COVID-19 pandemic reduced the bureau's funding by approximately 30 percent. The reduction had a ripple effect throughout the bureau, resulting in less funding to hire personnel to carry out its work.[64]

  Officials from the Bureau of Budget and Planning stated that IT system owners at bureaus are responsible for prioritizing their budget requests and for fulfilling cybersecurity requirements within available resource levels. While the Bureau of Consular Affairs faced budget constraints during the pandemic, it received $120 million in supplemental appropriations in fiscal year 2021 specifically to

[63]State's *Cyber Risk Management Strategy* defines "high risk" to mean that a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation. "Moderate risk" means that a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.

[64]Some bureau funding comes from fees generated through the issuance of passports, visas, and other documents. The decline in travel reduced funding from these sources. For example, as we reported in 2022, revenue for the Bureau of Consular Affairs decreased in fiscal year 2020 by 41 percent to $2.3 billion, in large part because of the pandemic. See GAO, *Consular Affairs: State May Be Unable to Cover Projected Costs if Revenues Do Not Quickly Rebound to Pre-Pandemic Levels*, GAO-22-104424 (Washington, D.C.: Apr. 18, 2022). Consular revenues in fiscal years 2020 through 2021 went up slightly, according to State's fiscal year 2021 financial report. Nonetheless, revenues in fiscal year 2021 were still less than fiscal year 2019. See Department of State, *Fiscal Year 2021 Agency Financial Report* (Washington, D.C.: Nov. 15, 2021).

enhance its IT platform by funding IT modernization projects that support consular systems. Officials added that the funding for the Bureau of Consular Affairs began to recover in fiscal year 2022, enabling sustained investments in IT and cybersecurity.

- **State's federated IT management structure:** Although IRM has the responsibility of managing the cybersecurity A&A process resulting in a system getting an ATO, many of the RMF steps are dependent upon coordination with bureau system owners. This is due, in part, to the federated nature of the department's IT management structure. According to the CIO, system owners delay completing those steps due to competing priorities. State's federated IT management structure makes it challenging to enforce the CIO's authority over the system authorization process. We provide more detail about the CIO's authority later in this report.

State officials stated that IRM had made strides toward improving the RMF experience for bureau system owners. State established the system owner support team in 2021 to assist system owners with completing RMF steps 1 through 3 and to ensure that they would be ready for assessments by validating data. This team provides support at no cost to bureaus to help address their lack of personnel resources. According to IRM officials, the available pool of RMF step 4 assessors was greatly expanded throughout 2022, more than doubling in size.

In addition, State has dedicated more A&A resources to better track RMF progress based on system owner feedback. According to State officials, the department has authorized about 72 percent of its information systems for operation through the A&A process, including HVAs. This was an increase of 16 percent from the prior year. However, State did not provide verifiable evidence that it had implemented the aforementioned activities.

Until State ensures that its IT and HVA systems are authorized to operate on its networks, the department will not have assurance that it is sufficiently aware of its risks and that security controls are operating as intended.

State Did Not Consistently Document Requirements for Information Security Continuous Monitoring

The NIST RMF specifies that an organization's continuous monitoring strategy should define and document the minimum monitoring frequency for implemented controls across the organization (including at the

department and information system levels).[65] Although the department's information security continuous monitoring (ISCM) strategy includes various ways of continuously monitoring security controls, it lacks definitive minimum frequency requirements for each method.[66] The strategy provides examples of minimum frequency for monitoring, but it specifies that information system owners must define the actual frequency.

Three system security plans from the seven selected systems specified a frequency for monitoring based on the schedule set for the iPost application.[67] However, plans for the four other systems did not specify minimum frequency requirements for monitoring. As a result, the department lacks a measurable method for how it will address monitoring requirements at the information system level.

State Has Not Fully Implemented Its Continuous Monitoring Program Department-Wide

State developed a strategy for implementing a continuous monitoring program for information security. Specifically, the department has implemented vulnerability monitoring of OpenNet via the iPost system and various monitoring tools for vulnerability data analysis. It then uses the data collected by the tools to respond to vulnerability findings.

However, according to IRM officials, the department has not implemented key capabilities of its ISCM program. For example, it has not implemented continuous diagnostics and monitoring.

According to officials, IRM is unable to fully implement capabilities for its continuous monitoring program because IRM cannot always access bureaus' assets. This is due in part to the bureaus owning and managing their own assets.

Officials stated that the department planned to begin monitoring these capabilities by the end of calendar year 2021 through its continuous

[65]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations*, Special Publication 800-37, revision 2.

[66]Department of State, *Information Security Continuous Monitoring Strategy*, version 1.4.

[67]iPost is a custom application developed and implemented by the department and is intended to provide continuous monitoring capabilities over selected elements of State's IT environment. Using data collected by various automated monitoring and management tools and a scoring method based on the premise that higher scores mean higher risk, the iPost risk scoring program is intended to provide local administrators and enterprise-level management with an improved capability to monitor and report on risks and risk mitigation efforts affecting the department's IT infrastructure.

diagnostics and mitigation dashboard. However, as of December 2022, the department has not provided evidence that the program had been fully implemented. Officials noted that the effort to catalog IT assets is a significant multi-bureau, department-wide effort and is taking longer than expected. Officials also stated that the capability for continuous diagnostics and mitigation asset management is 100 percent complete, and the capability for identity and access management is 82 percent complete, with an estimated completion date of March 17, 2023. However, State did not provide us with evidence of implementing these capabilities.

Until the department establishes a comprehensive, continuous monitoring program that includes continuous diagnostics and mitigation, it will be less able to effectively manage risks to its assets, system identity and access, and network and data security. Furthermore, the department will not have sufficient knowledge of information security vulnerabilities and threats affecting mission operations to ensure that department-wide operations remain within an acceptable level of risk.

State's Incident Response Process Aligns with Federal Guidance but Lacks Full Implementation and Secure IT Infrastructure

State's process for detecting, responding to, and recovering from cybersecurity incidents generally aligns with NIST's guidance on incident response.[68] This includes when to report the incident to US-CERT and how a cybersecurity incident should be handled from the beginning to its final resolution. Although State fully documented all the required information for 23 of 25 cybersecurity incidents, the department has not fully implemented all aspects of its incident response processes for detecting, responding to, and recovering from a cybersecurity incident. For example, State has not consistently conducted annual tests of its incident response procedures and has not fully updated or tested contingency plans for its information systems to ensure continuity of operations for its information systems. Additionally, until 2023, State had not provided guidance to its information system security officers about reporting incidents with sufficient details.

Further, State has not secured its IT infrastructure (i.e., its network and system hardware and operating system software) to support its incident response program. For example, State has not

- tracked all IT hardware and software,

[68]National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, revision 2 (Gaithersburg, MD: Aug. 2012).

- replaced outdated hardware and software on servers and network devices, nor
- captured network traffic data on its firewalls.

For this objective, we have omitted sensitive information that is contained in our August 2023 report.[69] The omitted information includes the identification of certain system names, specific technologies, and details concerning a specific weakness.

State Established Incident Response Processes That Were Generally Consistent with Federal Guidance

FISMA requires that federal information security programs include policies for detecting, reporting, and responding to security incidents.[70] According to FISMA requirements and NIST guidance, agencies should establish an incident response policy and require incident response testing.[71] FISMA requirements[72] and State policy[73] call for the department's federal information security programs to include procedures for detecting, reporting, and responding to security incidents. These procedures are to include processes for reporting incidents to US-CERT.

State's incident response policy generally aligns with federal guidance by requiring the department to establish an incident handling capability for its information systems. Specifically, the policy requires this capability to include adequate preparation, detection, analysis, containment, recovery, and user response activities. The policy also requires that the department track, document, and report incidents to appropriate internal and external authorities. In addition, State policy requires that bureaus and posts test the incident response capability at least annually.[74]

State established its Cyber Incident Response Team (CIRT) in 1998 in DS's Monitoring and Incident Response Division. This division is charged with deploying the capabilities necessary to defend over 125,000 assets at 270 overseas posts and 150 domestic offices. The division implements

[69]GAO-23-103834SU.

[70]44 U.S.C. §§ 3554(b)(7).

[71]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

[72]44 U.S.C. §§ 3554(b)(7).

[73]Department of State, *Foreign Affairs Handbook,* "Incident Response," 12 FAH-10 H-240 (Nov. 16, 2015). Note: This is an internal State document not available to the public.

[74]Department of State, *Foreign Affairs Handbook,* "Incident Response," 12 FAH-10 H-240.

cybersecurity policies and objectives for the department through three organizational units: the CIRT, the Red Cell, and Blue Team.[75]

Collectively, these units are to provide the capability to identify active and potential threats to network security 24 hours a day, 7 days a week. Additionally, these three units coordinate remediation to enhance the department's overall security posture. The CIRT serves as the central reporting point for cybersecurity incidents within State. DHS has designated the CIRT as the official conduit for reporting cybersecurity incidents to US-CERT on behalf of State. The CIRT shares security information with law enforcement entities as appropriate.

In addition, State policy requires that incident-handling capabilities for its information systems include adequate preparation, detection, analysis, containment, recovery, and user response activities.[76] For example, the CIRT's standard operating procedures state that the department is to conduct security monitoring of networks within State to ensure the integrity, availability and confidentiality of the IT infrastructure.[77] CIRT operations are to provide near real-time detection, collection, analysis, correlation, and reporting of cybersecurity events that pose a threat to the department's networks.[78] According to the procedures, the team is to coordinate with numerous components within State to remediate security events upon detection and report the overall status of the department's cybersecurity posture to senior management each business day.

Once the department identifies or reports such an event, the CIRT is to perform an assessment to determine if the event is a cybersecurity

[75]The CIRT is responsible for incident response network monitoring, malware analysis, advanced analytics development, threat integration and cloud. Red Cell is responsible for penetration testing. Blue Team provides vulnerability assessments and remediation support to department system owners and administrators to proactively enhance the ability of information technology systems to protect against exploitation attempts by advanced cyber threat actors.

[76]Department of State, *Foreign Affairs Manual*, "Unclassified Information System Security Policies," 12 FAM 620 (Aug. 11, 2017), https://fam.state.gov/FAM/12FAM/12FAM0620.html.

[77]Department of State*, Cyber Incident Response Team Standard Operating Procedures,* version 8.8 (Arlington, VA: May 10, 2022).

[78]The CIRT defines a cybersecurity event as "any abnormal occurrence or possible malicious activity on State's network."

incident and attempt to identify the cause.[79] If the CIRT determines an event not to be a cybersecurity incident, the team informs the entity that reported it. Subsequently, the team will either close the case or refer it to the responsible unit. Examples of events that are not incidents can include a user connecting to a file share, a server receiving a request for a web page, a user sending an email, and a firewall blocking a connection attempt.

According to DS officials, if a cybersecurity event is determined to be an incident, the department follows the CIRT's standard operating procedures. These procedures directly align with NIST guidance for the handling of an incident.

DS officials further stated that when an incident is deemed "significant," a specialized procedure called the significant incident response plan is triggered.[80] DS officials added that they leverage a prioritization scale that is similar to US-CERT's process in its National Cyber Incident Scoring System for assigning prioritization based on key factors of an incident.[81] In addition, according to DS officials, government leadership staff in DS's CIRT are trained and have experience in identifying events of particular interest or concern due to the department's unique attributes.

According to DS officials, either of these processes may warrant the reporting of an event to the point where the Director and Deputy Assistant Secretary leaders within DS / Cyber and Technology Security are briefed on it as part of a significant incident response plan. The CIRT then follows this plan for the duration of the significant cyber incident.

[79]An event is any observable occurrence in a system or network. A computer cybersecurity incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of a cybersecurity incident are an attacker commanding a botnet to send high volumes of connection requests to a web server, causing it to crash, and a user providing or exposing sensitive information to others through peer-to-peer file sharing services.

[80]Presidential Policy Directive/PPD-41, *United States Cyber Incident Coordination* (Washington, D.C.: July 26, 2016). The directive defines a significant cyber incident as an incident or group of related cyber incidents that are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[81]The National Cyber Incident Scoring System is designed to provide a repeatable and consistent mechanism for estimating the risk of an incident.

State Has Not Fully Implemented Its Incident Response Processes or Supporting IT Infrastructure

State has not fully implemented its incident response processes or the IT infrastructure that supports them. State generally documented all required information in its cybersecurity incident tickets, but it did not implement other incident response processes. Specifically, State has not consistently conducted annual testing of its incident response procedures and has not fully updated or tested contingency plans for its information systems. Moreover, the department lacked guidance about reporting cybersecurity incidents until State updated the communications and reporting sections of its significant incident response plan in 2023.

State Generally Documented All Required Information in Its Cybersecurity Incident Tickets

NIST Special Publication 800-53 states that agencies should document security incidents for information systems. For example, documentation involves maintaining records about each incident, including its status and other information necessary for evaluating incident details, trends, and handling.[82] A variety of sources can provide incident information, including the incident response team, incident reports, user and administrator reports, audit and network monitoring, and physical access monitoring.

According to State procedures, when incident handlers escalate an event to a cybersecurity incident, they must maintain a chronological log of events within the department's ticketing system. This log is an official record of activity and serves as the basis for developing any reports to management on incident handling. Reports of cybersecurity incidents should include a description of the incident using the appropriate classification; however, incident handlers should not delay reporting to gain additional information.

CIRT procedures require capturing the following specific information in the ticket:

- **Functional impact:** the current level of impact on agency functions or services
- **Information impact:** the type of information lost, compromised, or corrupted
- **Recoverability:** the estimated scope of time and resources needed to recover from the incident
- **Time:** when the activity was first detected or reported

[82]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

- **Number of impacted users:** the number of systems, records, and users impacted
- **Location:** the network location of the observed activity
- **Point of contact:** information on the individual who should be contacted for additional follow-up

Of the 25 selected incident response tickets from fiscal year 2019 through fiscal year 2021, 23 contained all the information as required by the CIRT's standard operating procedures. The remaining two tickets did not identify the type of information that was lost, compromised, or corrupted as required by the CIRT's procedures.

According to DS officials, at the time of those incidents, the department used an incident management tool that was the system of record for the CIRT and was to serve as the data repository of incidents for further discovery.[83] DS officials added that it was not possible to translate all the fields from its former incident response tool to its current incident response platform fields. Officials attributed this to the limited amount of time afforded for the transition and the loss of some data during the migration to the new platform.

Officials added that in October 2021, DS's CIRT transitioned to the current platform, which has more integration capabilities for incident management than the prior platform.[84] The integration of the current platform allows State to search through incident tickets to assess, detect, and intervene without the consistent need for human interaction. This can reduce the time needed to respond to an incident.

While the department largely documented the required information for the incidents we selected, not identifying the type of information that was lost, compromised, or corrupted could limit the department's ability to respond to cybersecurity incidents. In addition, State would have limited ability to determine incidents' root causes; to develop accurate, complete, and

[83]This incident management tool collects data in real time, allowing for each event and piece of data to be time stamped with the time and date it occurred. It also automates the sending of notifications, escalates tasks and alerts to the appropriate people, and helps prioritize the task or event.

[84]The platform allows for tools such as those that provide security information and event management to be integrated into the incident response process.

detailed time lines; to identify when the department first detected an activity; and to apply lessons learned to help prevent future incidents.

State Has Not Consistently Conducted Annual Testing of Its Incident Response Procedures

NIST guidance states that testing incident response capabilities can determine their overall effectiveness and identify potential weaknesses or deficiencies. For example, incident response testing can involve the use of checklists, walk-throughs or tabletop exercises, and simulations.[85] Incident response testing can help departments and agencies determine the effects of a response on their operations (e.g., reduction in mission capabilities), assets, and individuals.

State tested its incident response procedures, but at the time of our review, according to DS officials, the department had not consistently conducted tests annually as required by State policy. Specifically, State conducted a test of its incident response procedures in 2019. Subsequently, DS officials stated that they had planned to conduct a tabletop exercise to test its incident response procedures in 2020, but COVID-19 delayed it.

During our review, State completed testing its department-wide incident response procedures. In March 2022, the department completed a Cyber Storm VIII exercise coordinated by DHS.[86] The Cyber Storm VIII exercise served as an opportunity for DS's CIRT to test its incident response policies, processes, and practices. Specifically, the CIRT tested the department's response to threats from unauthorized access, compromised accounts, and compromised networks. According to State officials, the CIRT's adherence to its current standard operating

[85]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

[86]Cybersecurity and Infrastructure Security Agency, *Cyber Storm VIII: After-Action Report,* (Washington, D.C.: Aug. 2022). As an operations-based functional exercise, Cyber Storm VIII allowed participants to simulate their response to multiple concurrent cyber incidents. The exercise assessed cybersecurity preparedness; examined incident response processes, procedures, and information sharing; and identified areas for improvement. Cyber Storm VIII, held in March 2022, allowed over 2,000 participants to exercise their cyber incident response plans and identify opportunities for coordination and information sharing. Building on the success and momentum of Cyber Storm 2020 and lessons learned from real-world events, Cyber Storm VIII prepared participants to respond to emerging and evolving threats. Cyber Storm VIII was the first iteration of the exercise to be designated as the National Cyber Exercise per the requirements of Section 1744 of the Fiscal Year 2021 National Defense Authorization Act (Public Law 116-283, enacted Jan. 1, 2021).

procedures and applicable portions of the significant incident response plan helped the department to complete the exercise successfully.

Since the Cyber Storm VIII exercise, DS officials stated that they are working with CISA to perform testing of the bureau's incident response procedures in June 2023. However, they did not provide evidence of their schedule to test this capability. It is important that State establish a consistent schedule and process for testing its incident response capability annually to ensure that the department can effectively respond to incidents.

State Has Not Fully Updated or Tested Contingency Plans for Its Information Systems

FISMA requires federal agencies to develop and document plans and procedures to ensure continuity of operations for information systems that support their operations and assets.[87] According to NIST guidance, contingency planning is part of overall information system planning for continuity of operations. Such planning is essential for agencies to prepare for the loss of operational capabilities due to a service disruption, such as a cybersecurity incident that renders a system unusable.[88]

NIST guidance recommends that agencies develop, periodically review, and test a contingency plan for each system.[89] Consistent with NIST guidance, State requires annual updates and testing of contingency plans for its information systems.[90]

Although State developed contingency plans for all seven of the systems we selected for review, the department did not always update or annually test the plans for two systems. Specifically, State has not updated the contingency plan for one system since September 2019 and had not annually tested the plan for another system.

[87]44 U.S.C. § 3554(b)(8).

[88]National Institute of Standards and Technology, *Contingency Planning Guide for Federal Information Systems*, Special Publication 800-34, revision 1 (Gaithersburg, MD: May 2010).

[89]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

[90]Department of State, *Foreign Affairs Handbook*, "Contingency Planning," 12-FAH-10 H-230 (Jan. 24, 2017). Note: This is an internal State document not available to the public.

State also identified similar weaknesses in annual contingency plan updates and testing in the department's March 31, 2021, risk scorecard.[91] Specifically, the scorecard showed that State had not annually updated 211 or tested 239 of the contingency plans for its 484 information systems department-wide. More recently, State officials stated that they have made progress and that contingency plans for 149 systems remain untested. However, State did not provide us with verifiable evidence that it had completed these tests of its system contingency plans.

The scorecard also noted that the department lacked effective contingency plan testing for its HVA systems. For example, State has not conducted annual contingency plan testing for most of its FISMA reportable HVAs, and the scorecard did not document that some systems had tested a contingency plan.[92] Specifically, the scorecard

- documented that State had a current test of contingency plans for 13 percent of its HVA systems (i.e., no more than a year had passed since the last documented test),
- documented that State had not annually tested the contingency plans for approximately 77 percent of its HVA systems, and
- did not indicate if 10 percent of State's HVA systems had contingency plans and if those plans had been tested annually.

Officials from the Bureau of the Comptroller and Global Financial Services and the Bureau of Consular Affairs stated that, due to mission demands, most IT systems must be available at all times. Therefore, bureaus did not always power down systems periodically for contingency plan testing. Nevertheless, per NIST requirements, system contingency plans can be tested in various ways such as walk-through and tabletop exercises, checklists, and simulations, which do not require systems to be powered down.[93]

In December 2022, State officials stated that the department is making significant progress in testing its contingency plans. For example, officials

[91]The Global IT Risk Office issues bureau-level risk scorecards to communicate cybersecurity risks affecting bureaus at the department. The scorecard tracks assessment and authorization numbers and any contingency plan testing, HVAs, and other FISMA-related attributes.

[92]This information is based on State's risk scorecard data for its bureaus' HVAs (accessed on April 19, 2021).

[93]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

reported that State had tested contingency plans for all of its HVAs. Officials from the Bureau of Consular Affairs also asserted that the bureau conducts annual contingency plan tests for almost all its systems. However, the officials acknowledged that improvements are still needed, and the bureau is working to complete contingency plan testing for each of its systems. Further, State did not provide us with new evidence that it had tested its contingency plans.

Until State ensures that the contingency plans for its information systems are annually updated and tested, the department faces the risk that it will not be able to recover mission essential functions during a service disruption or ensure recovery activities are effective.

State Lacked Guidance until 2023 about Reporting Cybersecurity Incidents with Sufficient Details

NIST guidance states that agencies should establish how they should share cybersecurity incident information in an incident response plan.[94] Further, State[95] and GAO[96] internal controls guidance state that management should communicate quality information through established reporting methods at all levels of the organization on a timely basis.

In August and September 2021, ISSOs we interviewed at five of the overseas posts stated that the information they receive from IRM about cybersecurity incidents lacks enough detail to determine the extent to which incidents affect the systems and applications they manage. They stated that receiving such details could aid them in being able to better coordinate and more quickly mitigate incidents and prevent future activities that could compromise systems.

During our review in February 2023, DS made major revisions to its significant incident response plan, including updates to the communications and reporting sections of the plan. For example, these revisions specify that during and after an incident, a variety of communications products with varying restrictions on distribution based on sensitivity are provided to the appropriate stakeholders and partners, which include ISSOs at posts.

[94]National Institute of Standards and Technology, *Computer Security Incident Handling Guide*, Special Publication 800-61, revision 2 (Gaithersburg, MD: Aug. 2012).

[95]Department of State, *Foreign Affairs Manual*, "Management Controls," 2 FAM 020, (Feb. 25, 2019), https://fam.state.gov/FAM/02FAM/02FAM0020.html

[96]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 2014).

State Has Not Adequately Secured Its IT Infrastructure to Support Its Incident Response Program

State has not secured its IT infrastructure to support its incident response program. For example, State has not

- tracked all IT hardware and software,
- replaced outdated hardware and software on servers and network devices, and
- captured network traffic data on its firewalls.

State Did Not Track All of Its IT Hardware and Software

NIST guidance requires federal agencies to develop and document an inventory of information system components that accurately reflect current information systems.[97] This component inventory should include all components within the authorization boundary of the information system and contain the level of detail deemed necessary for tracking and reporting.[98]

However, State has not fully documented all of its information system components, including hardware and software, in its enterprise configuration management database. Specifically, the database only contained asset inventory information for one specific operating system from available inventory data sources on OpenNet—the department's enterprise network. In addition, State's network infrastructure was not implemented in a manner that would allow the database to capture configuration data from the hardware and software at 20 posts, resulting in an incomplete inventory of department network assets.

According to IRM officials, the database was updated during our review. The officials stated that, because of this update, the system is now able to discover and identify specific hardware and software not originally identifiable on OpenNet. However, the database is still only operational on OpenNet and is not available on other post networks, such as ClassNet or nonenterprise networks.

[97]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

[98]According to NIST, an authorization boundary includes all components of an information system authorized for operation by an authorizing official. This excludes separately authorized systems to which the information system is connected.

According to department officials responsible for security on post networks, each post is responsible for its own network. Since the post networks we reviewed do not connect to OpenNet directly, and post staff often manage the networks independently from the department, the database is not able to track department IT assets on post networks.[99] Further, an IRM official stated that the bureau is often not aware of all post IT assets and cannot effectively assist in the management of risks or the detection and response of cybersecurity incidents associated with those assets.

By not having complete and accurate hardware and software inventories, State cannot accurately manage risk on its networks, nor quickly and effectively respond to cybersecurity incidents. For example, the department would not be able to enforce software restriction policies relating to which authorized software can run on networks owned and operated by State. Unauthorized hardware and software may introduce vulnerabilities into State networks that may compromise the security of the systems and data residing on those networks. We intend to issue a separate report with limited distribution to describe in more detail the specific control weaknesses related to State's IT inventory management and our recommended actions.

State Did Not Always Replace Outdated Hardware and Software

NIST guidance recommends that agencies replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer.[100] This condition is often referred to as "end-of-life" (EOL). Furthermore, a June 2020 memo from State's CIO required department system owners to submit IT modernization and

[99]According to NIST, logical network separation can be enforced either by encryption or network device-enforced partitioning. National Institute of Standards and Technology, *Guide to Industrial Control Systems (ICS) Security,* Special Publication 800-82, revision 2 (Gaithersburg, MD: May 2015). State is using network devices to segregate OpenNet from the networks located on foreign posts. These network devices, though physically connected, restrict network communications creating logical network boundaries between OpenNet and post networks.

[100]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

mitigation plans outlining the removal of EOL technology products from system inventories.[101]

Hardware or software products that have reached EOL no longer receive security patches and updates to address security vulnerabilities. Hackers, nation states, and other adversaries actively work to compromise and penetrate federal government networks through these unpatched security vulnerabilities. The continued use of EOL technology products on the department's networks poses multiple cyber risks, including the possibility of a network breach, resulting in stolen identity credentials, removal of the department's sensitive data and personally identifiable information, and disrupted access to systems. However, State uses hardware and software that have reached EOL. Specifically, its enterprise configuration management database identified 23,689 hardware systems and 3,102 occurrences of network and server operating system software installations that have reached EOL.

According to the last two FISMA audit reports (September 2022 and October 2021) from State's Inspector General, the department consistently faced several challenges in maintaining up-to-date hardware and software inventories.[102] By not having accurate inventories, State may not be fully aware that these systems are EOL and require updating or replacement. Furthermore, IRM and post officials stated that COVID-19 adversely affected their ability to send technical experts to posts to update their devices. In addition, ISSOs at three of the 16 post locations and at one of the bureaus we reviewed stated that they lacked the technical expertise to update and configure their network devices to comply with DS's configuration policy found in the *General Layer 2 Switch Configuration Security Configuration Standard*.[103]

[101]Department of State, *Reminder of Requirement to Remove End-of-Life Technology Products from System Owner Inventories on the Unclassified Enterprise Network* (OpenNet), memorandum for the IT Executive Council from CIO Stuart McGuigan (Washington D.C.: June 1, 2020). Note: This is an internal State document that is not available to the public due to the sensitive information it contains.

[102]Department of State, Office of Inspector General, *Audit of the Department of State FY 2022 Information Security Program*, AUD-IT-22-43 (Sept. 2022); and *Audit of the Department of State FY 2021 Information Security Program*, AUD-IT-22-06.

[103]Department of State, Bureau of Diplomatic Security, *General Layer 2 Switch Configuration Security Configuration Standard,* version 2.1 (Washington, D.C.: Oct. 2019). Note: This is an internal State document that is not available to the public due to the sensitive information it contains.

IRM officials acknowledged that regional ISSOs who have additional technical expertise could support post ISSOs by guiding them through the steps needed to correctly configure and update network devices. This could reduce the risk of potential incidents on post networks. Officials stated that only one of the four regional information management centers has been funded to provide technical support to ISSOs at posts, but two others are being funded for this purpose. The officials added that the ability to coordinate remediation efforts among DS, IRM, and the posts is adversely affected by State's federated IT infrastructure and intricate management structure.

Until State updates outdated or unsupported products, its IT infrastructure is vulnerable to exploits, including unauthorized access to systems, elevation of privileges, and denial-of-service attacks. We intend to issue a separate report with limited distribution to describe in more detail the specific control weaknesses related to State's outdated hardware and software and our recommended actions.

State Did Not Capture Network Traffic Data

NIST guidance recommends that organizations establish automated mechanisms that collect and analyze data for increased threat and situational awareness. Additionally, the guidance requires organizations to increase their situational awareness through monitoring network boundaries and internal network traffic to identify inappropriate or unusual activity.[104] This helps an organization determine what events occurred within its systems and networks when investigating a cybersecurity incident.[105]

However, State did not enable available automated monitoring capabilities to analyze network traffic. Specifically, State did not configure the firewalls that we reviewed to capture sufficient information about network traffic.

Without capturing this information, the department will be hampered in detecting and thoroughly investigating cybersecurity-related incidents occurring inside their networks over an extended period, such as anomalous lateral movement. It is important to detect such incidents

[104]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

[105]Events could include lateral movement, breaches, malware infection, data exfiltration, and command and control.

early, as an attacker could use network discovery to target additional hosts for compromise, potentially leading to data exfiltration and other malicious activities. We intend to issue a separate report with limited distribution to describe in more detail the specific control weaknesses related to State's logging capabilities and our recommended actions.

State's Implementation of a Federated Structure Has Limited the CIO's Ability to Secure Systems

The CIO oversees the management of State's IT systems. However, these responsibilities are shared with the Bureau of Diplomatic Security (DS) and others due to State's federated IT structure, which limits the CIO's ability to effectively oversee the department's IT security posture. In addition, lack of communication due to State's insulated culture has also limited the CIO's ability to effectively oversee the department's IT security posture.[106] State's insulated culture has also contributed to a lack of clear communication on IT-related requirements to ISSOs at posts, interfering with the proper implementation of security controls.

For this objective, we have omitted sensitive information that is contained in our August 2023 report.[107] The omitted information includes the identification of certain system names.

State Took Steps to Improve the CIO's Ability to Secure IT Systems

Since 1996, various laws and federal guidelines have served to clarify and strengthen the role of the CIO. For example, the provisions commonly referred to as FITARA require State and other covered agencies to ensure that their CIOs have a significant role in the decision-making processes for IT budgeting, management, governance, and oversight.[108] Under State's policies, the CIO is responsible for managing and overseeing the department's cybersecurity program.

In the last several years, State has taken a number of steps to clarify and strengthen the roles of the CIO. In March 2019, the Secretary of State signed a memorandum that granted the CIO the authority to manage

[106]State refers to its "insulated culture"—i.e., bureaus operating independently—in its cybersecurity strategy when describing factors that caused implementing effective communications and data sharing protocols across the department to meet with varying degrees of success. See Department of State, Office of the Chief Information Security Officer, *Department of State Cybersecurity Strategy, FY 2019 – FY 2022*.

[107]GAO-23-103834SU.

[108]Provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (2014).

department-wide IT policy and implementation.[109] According to State's *Foreign Affairs Manual*, the CIO is to advise senior management on the acquisition, development, implementation, and secure operation of the department's IT systems.[110] As such, the CIO's duties include

- approving the development of State's *Cyber Risk Management Strategy* and IT strategic plan;
- overseeing cybersecurity activities throughout the department;
- providing support to bureaus and posts in securing their IT systems from unauthorized intrusions, as well as in the recovery of systems when intrusions occur;
- serving as the principal IT adviser to the Secretary of State, the Deputy Secretary for Management and Resources, the Under Secretary for Management, and other senior officials on matters involving the development, implementation, and revision of IT policies, plans, budgets, and programs;
- overseeing all IT procurements, and approving all IT purchases over $10,000;
- assessing and authorizing all information systems at the department; and
- managing OpenNet through IRM.

To help the CIO elevate the importance of cybersecurity throughout the department, in September 2020, the Under Secretary for Management created the following within IRM:

- **The Enterprise Chief Information Security Officer (E-CISO) and E-CISO office.** The E-CISO reports directly to the CIO and is primarily responsible for coordinating and managing State's cybersecurity program. This includes ensuring that cybersecurity budget requests are adequate and appropriate for IT activities throughout the department and using those requests to develop a department-wide

[109]Department of State, Secretary of State, *Delegation of Authorities to the Chief Information Officer* (Washington, D.C.: Mar. 25, 2019). Note: This State memorandum is not available to the public due to the sensitive information it contains.

[110]Department of State, *Foreign Affairs Manual,* "Bureau of Information Resource Management (IRM)," 1 FAM 270 (Feb. 17, 2022), https://fam.state.gov/FAM/01FAM/01FAM0270.html.

cybersecurity budget plan. Further, the E-CISO manages cybersecurity policy, procedures, and practices.

IRM officials said that the E-CISO position was created due to concerns that the official serving as Chief Information Security Officer—the position now occupied by the E-CISO—did not have sufficient authority and visibility to oversee cybersecurity activities throughout State. According to IRM officials, the prior Chief Information Security Officer did not report directly to the CIO, and the creation of the E-CISO position elevates the cybersecurity function.

- **Office of Global Information Technology Risk.** This office reports to the E-CISO. According to the E-CISO, it provides guidance for IT system owners at State to conduct their own IT risk assessments. In addition, the office is to provide insight into how risks associated with systems or applications affect others within State.

In October 2020, the Under Secretary for Management issued a memorandum reaffirming that the CIO is to oversee the department's overall cybersecurity program.[111] The main purpose of the memorandum was to clearly outline the roles and responsibilities of the CIO, E-CISO, and DS.

The memorandum included a matrix that described 13 cybersecurity functions, the key activities for each function, and the office or individual accountable or responsible for each activity.[112] While the CIO is accountable for the majority of the 13 functions, the CIO and DS share accountability for one of the functions—cybersecurity operations. Moreover, the CIO and DS share responsibility for implementing many activities needed to complete each function. For example, within the cybersecurity operations function, the CIO is accountable for activities such as managing the CIRT's network intrusion detection, security monitoring, and incident handling and response. However, DS is accountable for producing cyber threat advisories and comprehensive threat assessments. In addition, bureaus such as the Bureau of Consular Affairs are independently responsible for performing certain cyber activities. Appendix III provides a table showing the breakdown of the

[111]Department of State, Under Secretary for Management, *Department Cybersecurity Roles and Responsibilities 2020 and Beyond*.

[112]Officials who are accountable for a function or activity have the authority to make decisions and are ultimately answerable to senior officials at State—such as the Under Secretary for Management and, ultimately, the Secretary—for the correct and thorough completion of the task.

cybersecurity functions, their associated activities, and levels of responsibility for the CIO, E-CISO and others throughout State.

In October 2021, the CIO noted that State needed to update and operationalize the October 2020 matrix to further codify the roles of the E-CISO and others to better reflect specific cyber functions and activities that department leadership and bureaus engage in throughout State.

The CIO's Ability to Effectively Manage Cybersecurity Is Limited by Bureaus' Independent Responsibilities and Insulated Culture

NIST guidance states that three structures can be used to meet IT organizational needs: (1) centralized, (2) decentralized, and (3) hybrid.[113] The guidance further states that the appropriate governance structure for an organization varies based on factors such as mission or business needs, the culture and size of the organization, and the geographic distribution of the organization's operations, assets, and individuals. A hybrid structure is equivalent to the "federated" IT approach that State has implemented. According to NIST, this structure requires strong, well-informed leadership for the organization as a whole and for subordinate organizations. Additionally, a hybrid structure requires an understanding of cultural constraints that can limit the CIO's visibility into mission-related systems. State[114] and GAO[115] internal control guidance emphasize the importance of considering how units interact to fulfill their overall responsibilities, while FISMA delegated to the agency's CIO (or comparable official) the authority to ensure compliance with FISMA requirements.[116]

In State's federated IT structure, the CIO through IRM plays the central role in directing and managing State's cybersecurity functions and activities, but DS and the bureaus also play major roles. As such, each of the components for the department's IT security program contains

[113]See National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View,* Special Publication 800-39 (Gaithersburg, MD: Mar. 2011). In a centralized structure, the authority, responsibility, and decision-making power are vested solely in central bodies, while in a decentralized structure the governance structures, authority, responsibility and decision-making power are vested in and delegated to individual subordinate organizations. In a hybrid structure, the authority, responsibility and decision-making power are distributed between a central body and individual subordinate organizations.

[114]Department of State, *Foreign Affairs Manual,* "Management Controls," 2 FAM 020.

[115]GAO-14-704G.

[116]As discussed earlier, we did not do a full review to determine the extent to which State's funding policies and procedures adhere to the requirements in FITARA.

numerous requirements and interdependent activities that must flow seamlessly among IRM, DS, and other bureaus and offices.

However, State's cybersecurity strategy noted that the department's federated structure and insulated culture have created challenges in State's implementation of its IT security programs. State's federated IT structure has enabled some bureaus to independently purchase their own equipment, manage their IT systems, and fund their own IT—including equipment, software, and services. According to IRM officials, these actions may occur without the approval or knowledge of the CIO, particularly at the post level.

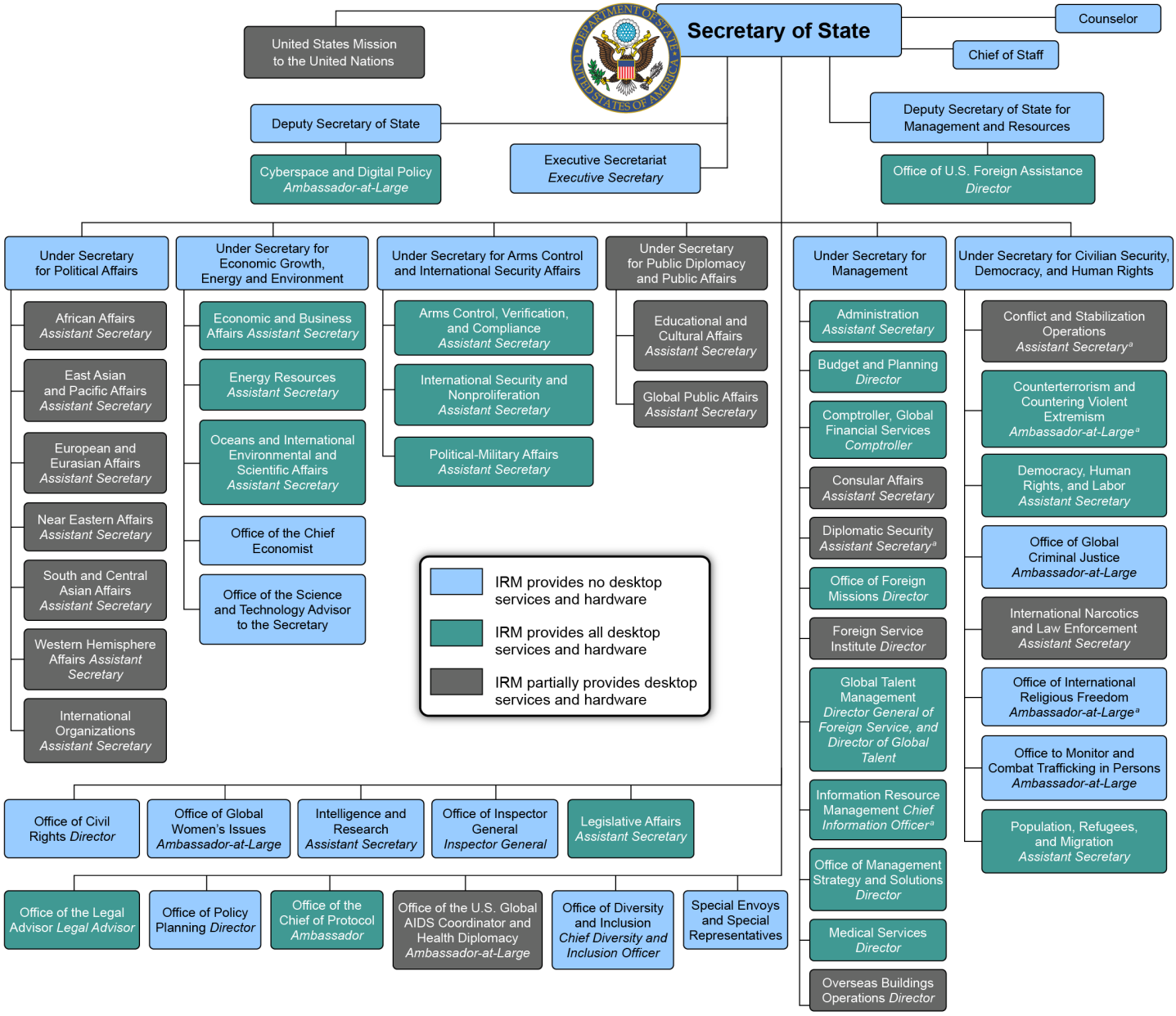
Bureaus Purchase Much of Their Own IT Equipment

Because State's purchasing authority is not centralized, some bureaus purchase their own IT equipment without the approval or knowledge of the CIO. For example, of State's 63 bureaus and offices, 22 rely on IRM for all purchases of IT desktop hardware, software, and services; 18 rely on IRM for some purchases, but not others; and 23 do not rely on IRM for these purchases at all.[117] Figure 2 shows the extent to which bureaus rely on IRM for the purchase of centralized IT desktop hardware, software, and services.[118]

[117]In this analysis, we counted the total number of business units, including the Office of the Secretary. To simplify the analysis, we counted the offices of the special representative and special envoys as one unit. None of the offices of the special representatives and special envoys receive centralized IT desktop services and hardware from IRM.

[118]Figure 2 presents a snapshot of the extent to which bureaus and offices rely on IRM for desktop hardware, software, and services as of May 2022. State's current organizational chart differed from the one presented in two ways: (1) the Bureau of Counterterrorism and Countering Violent Extremism was moved to the Under Secretary for Political Affairs, and (2) two offices—the Office of Global Partnerships and the Office of Global Food Security—were placed under the Under Secretary for Economic Growth, Energy, and the Environment.

Figure 2: Variations in State's Use of the Bureau of Information Resource Management (IRM) to Purchase Centralized IT Desktop Hardware, Software, and Services



Sources: GAO (analysis of Department of State documentation); State (logo). | GAO-23-107012

[a]The heads of these organizations report directly to the Secretary for certain purposes related to their assigned missions. For example, according to State officials, the CIO within IRM and the Assistant Secretary of DS have the authority to report directly to the Secretary on cybersecurity/IT matters.

IRM's *Functional Bureau Strategy* for fiscal years 2018 through 2022 noted that its IT service offerings are limited, causing some bureaus to acquire their own IT capabilities.[119]

State's lack of a centralized purchasing authority for IT equipment and services means that purchasing actions can occur without the approval or knowledge of the CIO. In August 2021, State's OIG found that IRM has designed and implemented a process to review and approve bureau-funded IT contracts,[120] but not all IT procurements valued at over $10,000 were appropriately routed to the CIO for review and approval per FITARA[121] and OMB requirements.[122] Specifically, program offices within bureaus were not appropriately identifying some procurements as IT-related. The OIG concluded that the CIO might not be afforded the opportunity to review and approve all IT procurements as required until additional actions were taken. In addition, the OIG also concluded that IRM would not be able to fully identify duplicative systems and related cost-saving opportunities, optimize its IT investments, or promote shared services.[123]

Bureaus Manage Many of Their Own IT Systems

Some bureaus independently manage their own IT systems; 22 of the department's 63 bureaus and offices also have IT offices to manage these systems. In addition, as discussed earlier, the October 2020 memo issued by the Under Secretary for Management assigned some

[119]Department of State, Bureau of Information Resource Management, *FY 2018-2022 Functional Bureau Strategy,* (Washington, D.C.: Nov. 9, 2018). Note: This is an internal State document that is not available to the public due to the sensitive information it contains.

[120]FITARA requires covered agency CIOs to annually review and approve agency IT investment portfolios. To assist the CIO in carrying out these responsibilities, State established two groups—an IT Executive Council directed by the CIO and an IT Executive Council Program Management Office. The IT Executive Program Management Office is charged with assisting in IT project proposal identification, review, and recommendation. For additional information about how State is organized to procure IT systems and challenges, see Department of State Office of Inspector General, *Compliance Follow-up Audit of the Department of State Process to Select and Approve IT Investments,* AUD-IT-21-34 (Arlington, VA: Aug. 2021).

[121]40 U.S.C. § 11319(b).

[122]Office of Management and Budget, *Managing Information as a Strategic Resource,* OMB Circular A-130 (July 28, 2016). Also see Office of Management and Budget, *Preparation, Submission, and Execution of the Budget,* OMB Circular A-11 (July 2020).

[123]See Department of State Office of Inspector General, AUD-IT-21-34. State's OIG made four recommendations in this report; as of March 2023, one had been closed and three were in the process of being closed.

cybersecurity responsibilities to individual bureaus such as the Bureau of Consular Affairs.[124]

Bureaus are responsible for cybersecurity activities that include

- maintaining an accurate inventory of bureau-owned hardware and software at headquarters and at domestic and foreign posts;
- implementing certain aspects of the ATO process, such as the assessment of security controls to ensure they are operating as intended and determining, where appropriate, the measures needed to remediate IT security vulnerabilities;
- conducting bureau risk assessments;
- replacing or reducing the risk of outdated hardware and software;
- developing system security plans; and
- developing and managing contingency plans.

IRM Does Not Provide Funding for All Bureau IT Systems

According to State's fiscal year 2023 *Congressional Budget Justification*, aside from IRM, 10 of the 63 bureaus and offices received IT-related funding through an IT central fund in fiscal year 2022.[125] In addition, the Bureau of Consular Affairs receives IT funding from a different fund and has autonomy to procure mission-specific hardware and software largely independent of IRM.[126] Regional bureaus provide funding to posts for IT equipment and software.

Lack of Communication Limits the CIO's Ability to Effectively Manage Cybersecurity and Has Resulted in Policy Confusion

As discussed earlier, NIST guidance stresses the importance of communication in a federated IT structure. Although the CIO is responsible for overseeing State's entire IT infrastructure, State's insulated culture has contributed to a lack of communication that has also limited the CIO's ability to effectively manage cybersecurity. In addition, lack of communication about shared responsibilities has resulted in policy confusion among ISSOs.

[124]Department of State, Under Secretary for Management, *Department Cybersecurity Roles and Responsibilities 2020 and Beyond.*

[125]Department of State, Foreign Operations, and Related Programs, *Congressional Budget Justification Fiscal Year 2023* (Washington, D.C.). Offices receiving central funding included the Office of the Secretary and the Office of the Under Secretary for Management.

[126]Since 2013, the Bureau of Consular Affairs has derived its IT funding from fees charged for consular services.

State's Insulated Culture Contributes to a Lack of Communication

State's insulated culture contributes to a lack of communication, which complicates the CIO's efforts to effectively manage cybersecurity. For example, officials from the Bureau of Consular Affairs noted that IRM has typically not provided common controls and other crosscutting capabilities needed by bureaus, and thus bureaus have had to figure this out for themselves.

To improve coordination of cybersecurity activities within the department, in October 2021, the CIO established a chief information security officer council, meeting once a month. As of April 2022, the council had met several times for different purposes, including meeting to announce and coordinate various cybersecurity initiatives such as the establishment of a cyber data strategy to address the department's struggles with data quality.

Lack of Communication about Shared Responsibilities Has Also Resulted in Policy Confusion

State[127] and GAO[128] internal controls guidance state that management should communicate quality information down and across reporting lines to help personnel perform key roles to achieve objectives and address risks. According to the guidance, management should select appropriate methods of communication.

State has not effectively communicated IT-related requirements to ISSOs at overseas posts so that it is clear how the CIO, IRM, and DS share IT responsibilities and when DS's guidance is applicable. According to the 2020 memorandum, the CIO is accountable for managing the department's cybersecurity program; however, DS is responsible for developing standards and guidelines that other bureaus and posts must use in configuring switches and systems. DS issued minimum standards for the security configuration of network devices (e.g., network switches) at bureaus and posts.[129] However, ISSOs typically follow IRM guidance. As previously discussed, as a result of a lack of clear communication, ISSOs have stated that they were unaware of the applicability of these standards because they had been issued by DS and not IRM.

IRM and DS officials said that they do not have difficulties communicating cybersecurity policies with each other. However, ISSOs being unaware that guidance existed outlining the minimum configuration settings

[127]Department of State, *Foreign Affairs Manual,* "Management Controls," 2 FAM 020.

[128]GAO-14-704G.

[129]Department of State, Bureau of Diplomatic Security, *General Layer 2 Switch Configuration Security Configuration Standard,* version 2.1.

indicates that the communication of technical requirements has not been effective.

IRM officials stated that they had informed ISSOs of the requirement to comply with DS guidance, but they acknowledged that they could do more. Officials also stated they could provide more support to ensure that security configurations are implemented appropriately. Without communication that is more effective regarding the applicability of policies and procedures across the department, the CIO will not be able to ensure bureaus and posts implement guidance related to the secure operation of IT systems as required. As a result, there is increased risk that the department's IT systems and devices will remain vulnerable to exploitation.

State's Implementation of Its Federated Structure and Lack of Communication Are Key Factors in Its IT Deficiencies

Although the CIO is responsible for overseeing all of State's IT infrastructure, many of the deficiencies identified in this report are the result of the CIO's lack of visibility into IT activities department-wide as well as a lack of communication. For example, as discussed previously:

- The federated nature of State's IT structure limits the CIO's ability to effectively manage the department's ATO process, which has resulted in approximately 265 State systems in bureaus and offices outside of IRM having expired ATOs according to the department's March 2021 bureau scorecard.
- The lack of a centralized inventory management system at the department level limits the CIO's ability to proactively identify hardware and software that have reached end-of-life but are still operating on State's network.
- A lack of communication limits the CIO's ability to ensure ISSOs carried out their responsibilities. Although IRM is responsible for managing the ISSO program, ISSOs in the Bureau of Consular Affairs report directly to Consular Affairs and not to IRM. At posts, ISSOs report to more senior management and not to IRM. In December 2020, State's OIG found continued deficiencies in the way ISSOs were performing their duties due, in part, to lack of management

oversight stemming from State's complex reporting structure. This placed State's computer systems and data at risk.[130]

- As discussed earlier, while State's enterprise configuration management database has been updated, it is not available on nonenterprise networks or post networks. Thus, State is still unable to track all of its hardware and software. Consequently, the CIO cannot readily access inventory data. According to IRM officials, State's slow implementation of the database is the result of IRM's having to negotiate with other bureaus to obtain access to their hardware asset data.

Failure to mitigate the cybersecurity deficiencies discussed in this report increases the risk that sensitive information could be disclosed or compromised. Therefore, until the CIO evaluates how State's IT cybersecurity responsibilities best support its federated IT infrastructure, the department may continue to have difficulties in securing its networks, systems, hardware, and software from security vulnerabilities that can be easily exploited.

Conclusions

Securing the information and systems that support State's mission is crucial to the department's ability to effectively manage its cybersecurity risks. State has taken some important steps in this direction. However, it has not fully implemented a continuous monitoring program or an information security continuous monitoring strategy. These and other deficiencies in the department's cybersecurity risk management program—such as a lack of bureau-level risk assessments and authorizations to operate for its information systems—limit State's ability to fully understand its risk posture. Until State addresses the deficiencies, it may face challenges in detecting and responding to security threats.

Although State has policies and processes to respond to cybersecurity incidents, it has not fully implemented incident response processes or secured its IT infrastructure, which makes State more vulnerable to malicious attacks. In addition, the department still uses hardware and

[130]See Department of State, Office of Inspector General, *Management Assistance Report: Continued Deficiencies in Performance of Information Systems Security Officer Responsibilities at Overseas Posts*, ISP-21-07 (Arlington, VA, Dec. 2020). This report resulted in a recommendation for State to conduct an organizational assessment of the ISSO program to determine the feasibility of creating full-time ISSO positions along with the appropriate reporting structure for personnel in these positions. In March 2022, State issued a report recommending that State increase the number of dedicated ISSO positions and have them report directly to IRM. However, it did not result in any recommendations to change the reporting structure for post ISSOs.

software that the vendor no longer supports and lacks automated capabilities to analyze network traffic. All of these deficiencies in infrastructure security controls limit State's ability to effectively detect vulnerabilities before they become incidents, respond to incidents when they do occur, and recover from those incidents successfully. Fully securing the IT infrastructure that supports its incident response program will better position the department to do appropriate forensic investigations and analyses.

Furthermore, State has clarified and strengthened the CIO's role within the department to better secure its IT systems, but bureaus' independent responsibilities—including those related to the procurement, management, and funding of IT systems—make it challenging for the CIO to effectively manage and oversee all aspects of its IT infrastructure. In addition, the department's difficulties effectively communicating IT-related requirements to posts to ensure their systems are secure leaves them vulnerable to exploitation. Until State resolves the CIO's information security limitations and rectifies security control deficiencies, the systems we reviewed and the sensitive information maintained on them will continue to face elevated and unnecessary risks.

Recommendations for Executive Action

We are making the following 15 recommendations to the Department of State:

The Secretary of State should direct the CIO to develop and maintain a department-wide risk profile that prioritizes the department's most significant risks, including the areas of exposure and threats that State identified, consistent with federal requirements. (Recommendation 1)

The Secretary of State should direct the CIO to develop plans to mitigate vulnerabilities in the areas of exposure and threats that State previously identified. (Recommendation 2)

The Secretary of State should direct the CIO to conduct bureau-level risk assessments for the 28 bureaus that owned information systems that we reviewed. (Recommendation 3)

The Secretary of State should direct the CIO to ensure that system security plans for the two systems we identified are updated at least annually as required by department policies. (Recommendation 4)

The Secretary of State should direct the CIO to ensure that State's information systems have valid authorizations to operate in accordance with department policies and federal guidance. (Recommendation 5)

The Secretary of State should direct the CIO to assess, prioritize, and allocate available department-wide resources to address the constraints that contribute to the backlog of its assessment and authorization process and coordinate these activities with the Bureau of Budget and Planning. (Recommendation 6)

The Secretary of State should direct the CIO to update the department's continuous monitoring strategy to define and document minimum frequency requirements for continuous monitoring of security controls and ensure the implementation of these requirements across department systems. (Recommendation 7)

The Secretary of State should direct the CIO to implement all components of State's Information Security Continuous Monitoring program across the department, including the continuous diagnostic and mitigation capabilities, in accordance with department policies and federal guidance. (Recommendation 8)

The Secretary of State should ensure that the CIO has access to assets at bureaus and posts to continuously monitor for threats and vulnerabilities that may affect mission operations. (Recommendation 9)

The Secretary of State should direct the Assistant Secretary of State for Diplomatic Security to ensure that State's incident response procedures are tested annually in accordance with department policies. (Recommendation 10)

The Secretary of State should direct the CIO to annually update the information system contingency plan for the one system we identified in accordance with department policies and federal guidance. (Recommendation 11)

The Secretary of State should direct the CIO to annually test the contingency plan for the one system we identified in accordance with department policies. (Recommendation 12)

The Secretary of State should direct the Assistant Secretary of State for Diplomatic Security to ensure that contingency plans for all HVA systems

are tested annually as required by department policies. (Recommendation 13)

The Secretary of State should direct the CIO to update the October 2020 matrix to better ensure compliance with applicable department policies and federal guidance. The update could involve operationalizing the matrix describing the roles and responsibilities of the various bureaus so that the department as a whole can better address cybersecurity requirements. (Recommendation 14)

The Secretary of State should direct the CIO and the Assistant Secretary for DS to ensure that IRM and DS provide more effective communication about the operation of IT systems to information system security officers at overseas posts regarding department policies and guidance. (Recommendation 15)

We previously published a version of this report with limited distribution due to the sensitive information it contained. Additionally, we 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.

Agency Comments

We provided a draft of this report to State for its review and comment. In its written comments, which are reprinted in appendix IV, the department concurred with all 15 recommendations we made to address cybersecurity weaknesses. State also provided technical comments in response to a draft of the sensitive version of this report. These included suggested wording changes to recommendations 6, 7, and 13, which we incorporated as appropriate. In addition, State described the steps planned or underway to address its incident response procedures. For example, the Bureau of Diplomatic Security stated that it will update its standard operating procedures for its cyber incident response program to formalize procedures related to annual reviews, updates, and testing activities.

We are sending copies of this report to the appropriate congressional committees, the Secretary of State, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Jennifer R. Franks at (404) 679-1831 or franksj@gao.gov, or Latesha Love-Grayer at (202) 512-4409 or lovegrayerl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Jennifer R. Franks, Director
Center for Enhanced Cybersecurity
Information Technology and Cybersecurity

Latesha Love-Grayer, Director
International Affairs and Trade

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine the extent to which (1) The Department of State has documented and implemented a program for cybersecurity risk management; (2) State has established and implemented a process and supporting infrastructure (IT assets and personnel with the necessary skills) 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.

This report is a public version of a sensitive report that we issued in August 2023.[1] State deemed some of the information in our August report to be sensitive, which we cannot disclose publicly. Therefore, this report omits the identification of post locations, certain system names, specific technologies, and a specific weakness from all three of our objectives. Although the information provided in this report is more limited, the report addresses the same objectives as the sensitive report and uses the same methodology.

As of June 10, 2021, State reported having 494 Federal Information Security Modernization Act of 2014 (FISMA) reportable systems connecting to its OpenNet Network Transport.[2] Of these reportable systems, 452 were sensitive but unclassified with low, moderate, and high impact ratings, including some systems designated as high value assets (HVA).[3]

[1]GAO, *Cybersecurity: State Needs to Implement Risk Management and Other Key Practices*, GAO-23-103834SU (Washington, D.C.: August 14, 2023).

[2]Systems subject to reporting under FISMA are categorized based on the potential impact on organizations or individuals in the event of a breach of security (i.e., loss of confidentiality, integrity, or availability). These numbers represent a snapshot in time and fluctuate weekly.

[3]According to Office of Management and Budget, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, M-19-03 (Washington, D.C.: Dec. 10, 2018), an agency may designate federal information or a federal information system as a high value asset (HVA) if it falls into specific categories outlined in M-19-03. While agencies are primarily responsible for designating systems as high value, the Office of Management and Budget and the Department of Homeland Security may also designate HVAs at agencies based on potential impact to national security.

To address our first two objectives, we selected a nongeneralizable sample of seven systems for review.[4] The department's main sensitive-but-unclassified network, OpenNet Network Transport, was selected due to the email breach that occurred in 2018.[5] Additionally, we selected six systems that reside on OpenNet. These six have centralized capabilities to detect, respond to, and recover from cybersecurity incidents.

To address our first objective—the extent to which State has implemented a program for cybersecurity risk management—we took the following actions:

- We identified and reviewed federal laws, policies, and guidance on cybersecurity risk management to identify risk management practices. These include federal laws, policies, and guidance enacted by Congress and the President, issued through executive orders by the White House, and issued by the Office of Management and Budget (OMB) and by the National Institute of Standards and Technology (NIST). We reviewed various policies and procedures such as the department's *Foreign Affairs Manual* and *Foreign Affairs Handbook*[6] to determine whether State had documented the roles, responsibilities, processes, and functions that the department must perform to manage cybersecurity risk consistent with Executive Order 13800.[7]
- We compared the department's *Cyber Risk Management Strategy* to OMB and NIST guidance to determine compliance with guidance and regulations on risk management related to cybersecurity risk. This

[4]Because we examined only seven of the 494 systems that State reported in its FISMA inventory with Federal Information Processing Standard (FIPS) 199 categorizations, the results of our review of system-level controls cannot be generalized to the entire State environment. See National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS Publication 199 (Gaithersburg, MD: Feb. 2004). The standard requires agencies to categorize each information system according to the magnitude of harm or impact should the system or its information be compromised. The standard defines three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

[5]State suffered a data breach that exposed employee data; the breach affected the department's unclassified email system in 2018, which is part of the OpenNet environment.

[6]Department of State, *Foreign Affairs Manual,* https://fam.state.gov/.

[7]The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

included (1) compliance as required under OMB guidance M-17-25[8] and (2) compliance with NIST guidance regarding the inclusion of the appropriate risk categories.[9] To do so, one GAO analyst reviewed relevant guidance and compared it to the *Cyber Risk Management Strategy* to determine whether the strategy aligned with federal standards. Then, a second analyst reviewed the first analyst's assessment of compliance. Where there were disagreements, they were resolved through discussion.

- We examined State's risk assessment documentation on its department-wide IT environment to determine if State conducted IT cybersecurity risk assessments at the department, bureau, and system levels. This documentation was provided to GAO in July 2021 and validated by the Office of Global Information Technology Risk (GITR). To conduct this review, one GAO analyst reviewed the relevant documentation and conducted the analysis. Then, a second analyst reviewed the first analyst's assessment. Where there were disagreements, they were resolved through discussion.
- We reviewed IT cybersecurity bureau-level risk assessments from the three bureaus that completed them to determine if they identified and addressed cybersecurity risks and prioritized risk management practices. We also reviewed the system security plans for the aforementioned seven selected systems. We compared the assessments and system security plans to the requirements laid out in NIST guidance.[10]
- We observed a demonstration of the risk management tools that the department uses to determine if they recorded, stored, and made decisions based on risks.
- We examined State assessment and authorization information for its FISMA-reportable IT systems based on a list provided by the

[8]Office of Management and Budget, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, M-17-25 (Washington, D.C.: May 19, 2017).

[9]Department of State, *Cyber Risk Management Strategy*, version 3.0 (Washington, D.C.: Aug. 2020). Note: This is an internal State document not available to the public.

[10]National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, MD: Apr. 2013) (withdrawn as of Sep. 23, 2021). For this audit, we evaluated State based on NIST 800-53 revision 4 since agencies had the option to adopt use of revision 5 immediately when it was finalized in September 2020 or continue to use revision 4 until it was withdrawn on September 23, 2021. Thus, for the majority of our audit, State was still using NIST 800-53 revision 4.

department, which included HVAs, to determine compliance with the department's Risk Management Framework (RMF).

- We assessed whether cybersecurity roles and responsibilities aligned with State's cyber risk management strategic plan by (1) reviewing documentation such as memos, charters, and strategies and (2) conducting interviews with officials from GITR and senior Information Resource Management (IRM) officials, including the CIO. Drawing on this information, one analyst assessed and classified staffing for these roles and responsibilities and confirmed the results through interviews with State officials. A second analyst reviewed the first analyst's assessment. Where there were disagreements, they were resolved through discussion.
- We assessed the department's implementation of the information security continuous monitoring (ISCM) program used to monitor OpenNet for vulnerability data analysis. As part of this assessment, one analyst conducted document reviews of State's cyber exposure report, ISCM strategic plan, and ISCM and continuous diagnostics and mitigation project plan to assess vulnerability monitoring. A second analyst reviewed the first analyst's assessments. Where there were disagreements, they were resolved through discussion. To further validate implementation of the program, we conducted interviews with the principal computer scientist in charge of the ISCM program and officials in IRM.[11]
- We assessed the completion of risk assessment scorecards at the bureau level. To do this, one analyst reviewed bureau risk assessments that GITR conducted and reported in bureau risk scorecards and evaluated them against OMB memorandums, NIST guidance, and the *Cyber Risk Management Strategy*.[12] A second analyst reviewed the first analyst's assessment. Where there were disagreements, they were resolved through discussion. We also interviewed officials from GITR to discuss the implementation and

[11]National Institute of Standards and Technology, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Special Publication 800-137 (Gaithersburg, MD: Sept. 2011).

[12]GITR issues bureau-level risk scorecards to communicate cybersecurity risks affecting bureaus at the department. The scorecard tracks assessment and authorization numbers and any contingency plan testing, HVAs, and other FISMA-related attributes.

challenges of completing bureau-level risk assessments department-wide.[13]

- We interviewed officials responsible for managing risk to obtain their perspectives on the department's implementation and challenges in complying with the NIST RMF[14] and State's risk management strategy.[15]

To address our second objective—the extent to which State has a process and supporting infrastructure (IT assets and personnel with the necessary skills) to detect, respond to, and recover from cybersecurity incidents—we identified systems that had interconnectivity with the department's main unclassified network, OpenNet. We identified systems that connected to OpenNet by conducting interviews with knowledgeable officials from State to understand the department's supporting IT infrastructure for its incident response program.

To understand the interconnectivity of State's network environment, we requested configuration files from 20 posts, but we only received configuration files from IRM and from post-managed network devices at 16 of the 20 posts reviewed.[16] We assessed State's compliance by comparing security settings with guidance from State's *General Layer 2 Switch Configuration Security Configuration Standard* and NIST guidance as criteria.[17] We intend to issue a separate report with limited distribution to describe in more detail the control weaknesses related to State's network environment and our recommended actions.

[13]A bureau-level risk assessment assesses the impact of system weaknesses to its mission operations. Such an assessment includes a business impact assessment that identifies likely threat sources and their likelihood of occurrence. The result identifies the level of risk a bureau faces arising from its reliance upon IT. Bureaus use this information to make risk decisions regarding specific bureau business process and system risk responses.

[14]National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, revision 2 (Gaithersburg, MD: Dec. 2018).

[15]Department of State, *Cyber Risk Management Strategy*, version 3.0.

[16]Because we examined configuration files from only 16 of State's 270 post locations, the results of our review cannot be generalized across all of State's networking environment.

[17]Department of State, Bureau of Diplomatic Security, *General Layer 2 Switch Configuration Security Configuration Standard,* version 2.1 (Washington, D.C.: Oct. 2019). Note: This is an internal State document that is not available to the public due to the sensitive information it contains.

The 16 posts selected for our nongeneralizable sample included one domestic post and 15 foreign posts. We selected the posts based on the following criteria:

- whether the location was a high/medium/low IT threat location
- whether an information system security officer, systems security engineer, or regional cybersecurity officer was present at a location
- the size of the post, its geographic location, whether the post was a major hub for activities (including IT activities State or other agencies conduct), and whether the post was the site of a Regional Information Management Center
- the manner in which IT activities were conducted and managed (which differed depending on whether the location was a domestic location or a post overseas and whether IRM or the posts themselves directly managed the switches)[18]

To further address objective 2, we reviewed and analyzed State's incident response policies and procedures to determine if they were consistent with State policy and NIST 800-61 and NIST 800-53 guidance.[19] Additionally, we interviewed key officials knowledgeable about the department's incident response program.

To determine if procedures and configurations complied with policies and regulations, one GAO analyst reviewed relevant procedures and configuration documentation and compared it to State and federal guidance. Then, a second analyst reviewed the first analyst's assessment of compliance. Where there were disagreements, they were resolved through discussion. Specifically, the reviews involved the following activities:

- We conducted a document review of State's incident response procedures to determine if they had been updated and tested

[18]To obtain the information needed to determine which locations to include in our fieldwork, we reviewed a number of reports that State, State's OIG, and GAO issued during fiscal years 2013 through 2021. We obtained most of the information used in making our determination from the State OIG reports, which documented the results of inspections conducted during fiscal years 2017 through 2021 at State locations both domestically and overseas.

[19]National Institute of Standards and Technology (NIST), *Computer Security Incident Handling Guide*, Special Publication 800-61, revision 2. (Gaithersburg, MD: Aug. 2012) and *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4.

according to 12 FAH-10 H-240.[20] We also examined contingency plans for the seven aforementioned selected systems, including HVA systems, to determine whether these plans had been developed, updated and tested as required by 12 FAH-10 H-240 and NIST guidance.

- We evaluated a sample of 25 incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT) to determine if the department had fully documented and reported them to US-CERT according to the standard operating procedures for the department's cyber incident response team.[21]
- We examined network device settings and network management servers to determine if they had been configured according to State's guidelines.

In addition, to determine how security plans and contingency plans for the selected information systems were used, one analyst examined and assessed whether those plans had been developed, updated, and tested. Then, a second GAO analyst verified the first analyst's assessment. To determine if network devices used multifactor authentication, one analyst manually reviewed the configuration files of network devices for the specification of authentication servers and a second GAO analyst verified the observation. Where there were disagreements, they were resolved through discussion.

Finally, we interviewed relevant security managers and response team members at State's Security Operations Center to better understand the capabilities and technologies in place to respond to and recover from cybersecurity incidents. Additionally, we interviewed cybersecurity response teams on whether State had sufficient qualified security experts and IT resources in place. We also interviewed department officials to determine the total number of outdated systems. State provided us with

[20]Department of State, *Foreign Affairs Handbook,* "Incident Response," 12 FAH-10 H-240 (Nov. 16, 2015). Note: This is an internal State document not available to the public.

[21]From fiscal year 2019 through March 2021, State reported that they submitted 3,910 tickets to the Department of Homeland Security. Of this total, State was able to retrieve/recover 3,474 tickets, which contained the summary ticket data. We worked with GAO methodologists to draw a nongeneralizable sample of 25 incidents. We selected incidents that did not include (1) anything categorized as an "event," (2) the unauthorized disclosure of classified information, or (3) unverified cases (explained anomaly). Additionally, we selected only those incidents that occurred on OpenNet and included cyber incident response team categories 1, 3, 4, 5, and 6. For the remaining cases, we sorted Resolution Category Tier 2 cases to create groupings from which to select our sample incidents.

the total of 245 systems, a number that the department validated before releasing it to GAO.

To address our third objective—to assess the extent to which State's CIO is able to secure its IT systems department-wide—we reviewed relevant documentation and reports and interviewed knowledgeable State officials. We interviewed the CIO, the Enterprise Chief Information Security Officer, the Assistant Secretary of Diplomatic Security (DS), and other relevant officials at State to understand how those roles and responsibilities were implemented and have changed since 2018. We interviewed State officials at one domestic and five foreign posts for these same reasons.

To identify and describe the CIO's cybersecurity roles and responsibilities and how State documented them, we reviewed and analyzed relevant reports from State's Office of the Inspector General (OIG), GAO, and others. To gain a better understanding of the CIO's role within the department related to IT, we examined State documentation. This included a March 2019 memo that granted the CIO the authority to manage implementation of department-wide IT policy and an October 2020 memo describing the CIO's roles and responsibilities.[22] To further validate our understanding of the CIO's ability to oversee the department's IT cybersecurity posture, we interviewed knowledgeable officials, including officials from IRM and DS.

As part of this review, one analyst reviewed State's policies and procedures and assessed whether the department documented them in accordance with federal laws and guidance. This included the Clinger-Cohen Act of 1996,[23] FISMA,[24] the provisions referred to as the Federal

[22]Department of State, Secretary of State, *Delegation of Authorities to the Chief Information Officer*, memorandum (Washington, D.C.: Mar. 19, 2019); and Department of State, Under Secretary for Management, *Department Cybersecurity Roles and Responsibilities 2020 and Beyond*, memorandum (Washington, D.C.: Oct. 22, 2020). Note: These are internal State documents that are not available to the public due to the sensitive information they contain.

[23]40 U.S.C. §§ 11312 and 11313.

[24]The Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073 (2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (2002). As used in this report, FISMA refers both to the 2014 act and to those provisions of the 2002 act that were either incorporated into the 2014 act or were unchanged and continue in full force and effect.

Information Technology Acquisition Reform Act (FITARA),[25] and Executive Order 13833.[26] A second analyst reviewed the first analyst's assessment, and where there were disagreements, they were resolved through discussion. However, we did not review the extent to which State's funding policies and procedures adhered to the requirements in FITARA. We also reviewed and analyzed reports from State's OIG, GAO, and others to document whether and how State has addressed any findings and recommendations regarding the CIO's authorities.

Lastly, we conducted virtual site visits to interview knowledgeable officials to understand how posts communicated and implemented IT security procedures. We selected a nongeneralizable sample of one domestic and five foreign posts based on the size of the post, threat potential of the location, whether the post had dedicated system security personnel on-site or was a regional information management center, and whether the post was a major hub for activities (including IT activities) conducted by State and other agencies.

To assess the reliability of information obtained from State, we interviewed knowledgeable officials from the Bureaus of IRM, DS, Consular Affairs, and selected domestic and overseas posts to corroborate the information we discovered in the data obtained. We found that the data we examined were sufficiently reliable for describing how State implemented its program for cybersecurity risk management and a process to detect, respond to, and recover from cybersecurity incidents as well as for describing the CIO's ability to secure State systems and factors that might limit the CIO's implementation of cybersecurity practices at the department.

We conducted this performance audit from October 2019 to August 2023 in accordance with generally accepted government auditing standards.[27] Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that

[25]The law commonly referred to as the Federal Information Technology Acquisition Reform Act (FITARA) consists of provisions of the Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, division A, title VIII, subtitle D, 128 Stat. 3292, 3438-50 (2014).

[26]The White House, *Enhancing the Effectiveness of Agency Chief Information Officers,* Executive Order 13833 (Washington, D.C.: May 15, 2018).

[27]During the period from March 2020 to November 2020, we made extensive adjustments to the schedule for this work due to the COVID-19 pandemic.

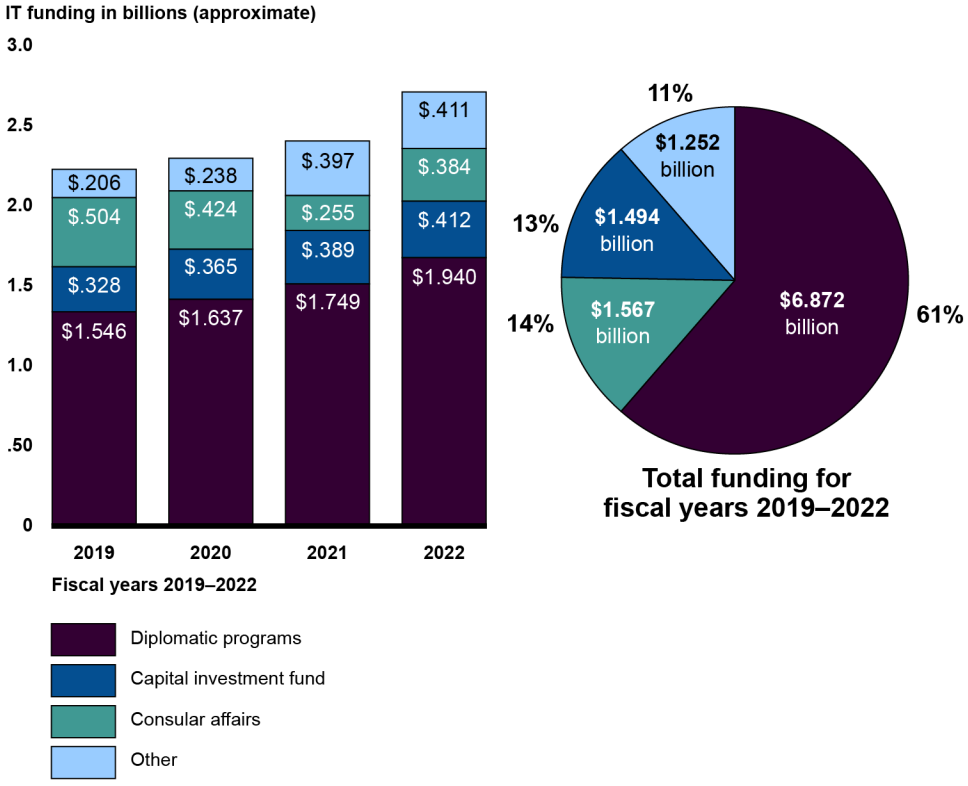
the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We subsequently worked with State from August 2023 to September 2023 to prepare this public version of the original sensitive report for public release. This public version was also prepared in accordance with these standards.

Appendix II: Department of State's IT Funding for Fiscal Years 2019–2022

The Department of State's funding for its IT infrastructure comes from appropriations and fees for four main funding sources: (1) the diplomatic programs account, (2) the capital investment fund, (3) funding for the Office of Consular Systems and Technology (a component of the Bureau of Consular Affairs), and (4) other sources of funding, such as State's working capital fund.[1] Overall, total funding for IT in fiscal years 2019 through 2022 was approximately $11.2 billion, of which about $1.7 billion was spent on cybersecurity. Figure 3 illustrates State's IT funding trends during these years according to State's Bureau of Budget and Planning.

[1]The diplomatic programs account funds the department's ongoing operations (including security), while the capital investment fund account funds the purchase of IT and other related capital investments. The consular systems and technology account funds IT investments and infrastructure for consular systems used both overseas and domestically. The "other" account includes funding derived from State's working capital fund. State generates funding for this account through an assessment of fees for the services it provides to agencies at overseas posts as well as through other funding sources.

Figure 3: State's IT Funding Trends from Appropriations and Fees, Fiscal Years 2019–2022



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

Appendix III: Cybersecurity Roles and Responsibilities of State's Bureaus and Offices

An October 2020 memorandum updated the division of responsibilities between the Bureau of Information Resource Management (IRM) and the Bureau of Diplomatic Security (DS).[1] It also assigned responsibilities for some activities to other bureaus.

The 2020 memorandum includes a matrix that lists 13 cybersecurity functions and 80 cybersecurity activities based on National Institute of Standards and Technology (NIST) guidance.[2] The activities consist of tasks needed to complete each function. For each function and related activities, specific levels of responsibility are assigned to IRM through the Chief Information Officer (CIO), Enterprise Chief Information Security Officer (E-CISO), and DS. The levels of responsibility are the following:

- **Accountable (A).** Officials have authority to make decisions and are ultimately answerable to officials at State who are more senior, such as the Under Secretary for Management and ultimately the Secretary of State, for ensuring the task is completed correctly and thoroughly.
- **Responsible (R).** Officials complete tasks.
- **Consulted (C).** Officials must be consulted regarding decisions and tasks.
- **Informed (I).** Officials are informed of decisions and tasks, with no expectation of a two-way discussion.

Table 5 provides a breakdown of the cybersecurity roles and responsibilities for the CIO, DS, E-CISO and others throughout State.

[1]Department of State, Under Secretary for Management, *Department Cybersecurity Roles and Responsibilities 2020 and Beyond* (Washington, D.C.: Oct. 22, 2020). Note: This is an internal State memorandum that is not available to the public due to the sensitive information it contains.

[2]National Institute of Standards and Technology, *Managing Information Security Risk: Organization, Mission, and Information System View*, Special Publication 800-39 (Gaithersburg, MD: Mar. 2011).

Table 5: October 2020 Breakdown of Cyber Roles and Responsibilities throughout State

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
Cybersecurity program management	Oversees State's cybersecurity efforts for all systems up to sensitive but unclassified	A	C	R-IRM (E-CISO)
	Oversees State's agency-wide information security program	A	C	R-IRM (E-CISO); I-Bureaus
	Manages CIO-assigned information security program functions with a primary focus on planning, building, running of technology programs, investments, and services	A	C	R-IRM (E-CISO)
	Manages CIO-assigned information security program functions with a primary focus on detect and respond activities	A	R	R-Bureaus with defensive cybersecurity activities
	Develops and manages State's agency-wide information security program plan as outlined in National Institute of Standards and Technology (NIST) guidance[a]	A	C	R-IRM (E-CISO); C-Information security program plan providers
	Ensures compliance with Federal Information Security Modernization Act (FISMA) provisions[b]	A	C	R-IRM (E-CISO)
	Manages State-wide cyber roles and responsibilities as components of the information security program plan, including memorandums of understanding between departmental entities and the E-CISO	A	C	R-IRM (E-CISO)
Cybersecurity portfolio management	Develops cybersecurity budgeting requirements	A	R	R-IRM (E-CISO); R-Any bureaus that receive funding for cybersecurity
	Ensures the adequacy of cybersecurity budget requests for activities across the department in alignment with mission goals	A	C	R-IRM (E-CISO); C-Any bureaus that receive funding for cybersecurity
	Oversees cyber elements of strategic capital planning and governance	A	C	R-IRM (E-CISO); C-Any bureaus that receive funding for cybersecurity
	Consolidates reporting regarding monetary spending and budgeting for cybersecurity activities	A	C	R-IRM (E-CISO); C-Any bureaus that receive funding for cybersecurity

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
Cybersecurity reporting	Manages all aspects of cybersecurity reporting	A	R	R-IRM (E-CISO); R-Any bureaus with cybersecurity reporting requirements
Cybersecurity risk management	Manages State's cybersecurity risk program	A	C	R-IRM (E-CISO); I-Bureaus
Cybersecurity policy	Manages cybersecurity policy, procedures, and practices	A	C	R-IRM (E-CISO); I-Bureaus
	Manages State's technology configuration standards	A	R	C-Bureaus
Cybersecurity governance	Manages IT and cyber governance	A	C	R-IRM (E-CISO); I-Bureaus
	Oversees IT supply chain risk management	A	C	R-IRM (E-CISO); R-Bureau of Administration (which provides support, including procurement, supply and transportation, diplomatic pouch and mail services, and language services) and all bureaus with IT systems C-Bureaus
Cybersecurity awareness, training, and workforce development	Manages cybersecurity awareness program	A	R	R-Foreign Service Institute
	Identifies training gaps	A	C	C-IRM; R-IRM (E-CISO)
	Develops role-based cybersecurity training requirements for technical and nontechnical skills	A	X	R-IRM (E-CISO)
	Develops role-based cybersecurity training	A	X	C-IRM (E-CISO); R-Foreign Service Institute
	Delivers role-based cybersecurity training	A	I	I-IRM (E-CISO); R-Foreign Service Institute
	Manages compliance with role-based cybersecurity training requirements	A	X	R-IRM (E-CISO); C-Foreign Service Institute

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
	Ensures relevant cybersecurity information is included in tradecraft courses	A	I	C-IRM (E-CISO); R-Foreign Service Institute
	Maintains and updates skill incentive programs for cybersecurity professionals	A	C	C-IRM (E-CISO); R-IRM
	Develops and delivers relevant cybersecurity contracts and acquisitions management training	A	X	C-IRM (E-CISO); R-Bureau of Administration
	Provides awareness and guidance for any individuals and groups involved in acquisition and management of cybersecurity contracts	A	C	C-IRM (E-CISO); R-Bureau of Administration
	Coordinates with stakeholders for department cybersecurity recruitment and retention efforts	A	C	C-IRM (E-CISO); R-IRM
High value asset	Manages high value asset (HVA) assessment program; HVAs are assets, federal information systems, and data for which unauthorized access, use, disclosure, disruption, modification or destruction could cause a significant impact to U.S. national security interests or to public confidence, among other things	A	C	R-IRM (E-CISO); C-Bureaus
Cybersecurity external representation	Representative to the Department of Homeland Security Cybersecurity and Infrastructure Security Agency's U.S. Computer Emergency Readiness Team (US-CERT)	A	R	C-IRM (E-CISO)
	Representative to the Department of Treasury with respect to cyber-related reviews	A	C	C-IRM (E-CISO); R-Process owner
	Representative to the Committee on National Security Systems on cybersecurity issues	A	C	R-IRM (E-CISO)
	Representative to the interagency community on cybersecurity issues	A	C	R-IRM (E-CISO)
	Coordinates cyber threat intelligence, sharing, and analysis	A	R	C-IRM (E-CISO)
	Participating member of the Chief Information Security Officer Council	A	I	R-IRM (E-CISO)
	Representative to the Office of Management and Budget on cybersecurity matters	A	C	R-IRM (E-CISO)

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
	Representative to NIST	A	C	R-IRM (E-CISO); C-Bureaus
	Representative to Congress on cybersecurity issues affecting State	A	C	R-IRM (E-CISO); C-Office of Legislative Affairs
	Representative to State's Office of the Inspector General on cybersecurity issues affecting State	A	C	R-IRM (E-CISO); C-Bureaus
Cybersecurity operations	Ensures State's compliance with cyber information security program requirements	A	C	R-IRM (E-CISO)
	Manages the Cyber Threat Program	I	A	R-DS; C-IRM (E-CISO); C-Bureau of Intelligence and Research
	Manages the Cyber Incident Response Team to include network intrusion detection, security monitoring, and incident handling and response	A	R	C-IRM (E-CISO); R-Bureaus with defensive cybersecurity activities
	Reports incident information to US-CERT	I	A	R-DS; C-IRM (E-CISO)
	Manages vulnerability and compliance testing	A	R	I-IRM (E-CISO)
	Conducts vulnerability scanning for inclusion in the department's risk-scoring program	A	R	I-IRM (E-CISO)
	Produces cyber threat advisories, special reports, and comprehensive threat assessments concerning threats to and potential vulnerabilities of State networks	I	A	R-DS; C-IRM (E-CISO)
	Leverages assessments of emerging technology to innovate new countermeasures and solutions to detect, defend against, and deter advanced cyber threats and enhance State's technical counterterrorism and counterintelligence capabilities	I	A	R-DS; I-IRM (E-CISO)
	Researches, develops, and maintains security configuration standards and principles for departmental implementation of IT hardware and applications	A	R	R-Bureaus; C-IRM (E-CISO)

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
	Conducts detailed vulnerability assessments involving specialized teams and regional cybersecurity officers to inform the calculation of risk and development of mitigation strategies; regional cybersecurity officers perform periodic assessments of State systems at posts to determine compliance with regulations	A	R	C-IRM (E-CISO)
	Provides specialized reviews to determine requirements for countermeasures both domestically and abroad	C	A	R-DS; C-IRM (E-CISO)
	Performs operational monitoring of networks and systems, manages communications security, and maintains technical security safeguards and mainframe security	A	I	C-IRM (E-CISO); R-IRM
	Performs security monitoring of networks	A	R	C-IRM (E-CISO); R-IRM
	Assesses emerging cybersecurity technology	A	R	I-IRM (E-CISO); R-IRM and DS
	Performs cybersecurity evaluations	A	R	I-IRM (E-CISO)
	Provides advanced threat hunting for anomalous traffic to identify threats and abnormalities on the network	A	R	I-IRM (E-CISO)
	Operates wireless intrusion detection system	A	R	C-IRM (E-CISO)
	Manages the information system security officer program; information system security officers are the designated officials to enforce information system security policies at the department	A	I	R-IRM
	Ensures site-based cybersecurity program effectiveness	A	I	R-IRM (E-CISO)
	Manages the antivirus program	A	I	C-IRM (E-CISO); R-IRM
	Oversees patch management	A	I	C-IRM (E-CISO); R-IRM
	Oversees enterprise configuration management (including standards)	A	C	C-IRM (E-CISO); R-IRM
	Collects and analyzes enterprise intrusion detection data	A	R	C-IRM (E-CISO)

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
	Analyzes, synthesizes, and reports cyber threat intelligence gathered through a variety of sources	I	A	I-IRM (E-CISO); R-DS
	Assesses targeting trends, indications, and warnings and develops reports and advisories for network defense resources	I	A	C-IRM (E-CISO); R-DS
	Develops security guides for major webmail and social media platforms to help State personnel recognize, report, and mitigate the targeting of online accounts	I	A	I-IRM (E-CISO); R-DS
	Manages public key infrastructure, which provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data	A	I	I-IRM (E-CISO); R-IRM
	Oversees electronic network key management	A	I	I-IRM (E-CISO); R-IRM
	Manages communications security	A	I	I-IRM (E-CISO); R-IRM
	Manages enterprise firewall infrastructure	A	I	C-IRM (E-CISO); R-IRM
	Manages Cyber Incident Response Team	A	R	C-IRM (E-CISO)
	Manages Virus Incident Response Team	A	I	C-IRM (E-CISO); R-IRM
	Develops system security plans	A	I	I-IRM (E-CISO); R-Bureaus
	Develops and manages contingency plans	A	I	I-IRM (E-CISO); R-Bureaus
	Develops self-assessments required under NIST SP 800-26[c]	A	I	C-IRM (E-CISO); R-Bureaus
	Conducts remediation management, including systems authorization as well as plans of action and milestones	A	I	C-IRM (E-CISO); R-Bureaus
	Manages plans of action and milestones not related to system authorization	A	I	R-IRM (E-CISO); I-Bureaus
Systems authorization	Manages the assessment and authorization process	A	I	R-IRM (E-CISO); I-Bureaus

Cyber function	Cyber activity	Role of Chief Information Officer (CIO)	Role of the Bureau of Diplomatic Security (DS)	Role of Bureau of Information Resource Management (IRM), Enterprise Chief Information Security Officer (E-CISO), and others
Cybersecurity architecture	Develops and implements an enterprise cybersecurity architecture	A	C	R-IRM (E-CISO)
	Leads continuous diagnostics and mitigation integration	A	C	R-IRM (E-CISO); C-IRM
Cybersecurity compliance	Manages program for cybersecurity compliance monitoring and enforcement	A	I	R-IRM (E-CISO)

Legend:

Accountable (A)–Officials have authority to make decisions and are ultimately answerable to officials at State who are more senior—such as the Under Secretary for Management and, ultimately, the Secretary—for completing the task correctly and thoroughly.

Responsible (R)–Officials complete tasks. We have separated the division of responsibilities within IRM between the E-CISO and other units within IRM.

Consulted (C)–Officials must be consulted regarding decisions and tasks.

Informed (I)–Officials are informed of decisions and tasks, with no expectation of a two-way discussion.

No Role (X)–Officials have no role in this cyber activity.

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

Note: Information in this table is from our analysis of Department of State, Under Secretary for Management, *Department Cybersecurity Roles and Responsibilities 2020 and Beyond*, memorandum (Washington, D.C.: Oct. 22, 2020). This State memorandum is not available to the public due to the sensitive information it contains.

[a]See National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, revision 4 (Gaithersburg, MD: Apr. 2013) (withdrawn as of Sept. 23, 2021).

[b]The Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, 128 Stat. 3073 (2014) largely superseded the Federal Information Security Management Act of 2002, enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, title III, 116 Stat. 2899, 2946 (2002).

[c]National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology* Systems, Special Publication 800-26 (Gaithersburg, MD: Nov. 2001). This reference in State's document is to a NIST publication that was withdrawn in December 2007.

Appendix IV: Comments from the Department of State

United States Department of State
Comptroller
Washington, DC 20520

SEP 15 2023

Jason Bair
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Mr. Bair:

We appreciate the opportunity to review your draft report, "CYBERSECURITY: State Needs to Expeditiously Implement Risk Management and Other Key Practices" GAO Job Code 107012.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

Sincerely,

James A. Walsh

Enclosure:
As stated

cc: GAO – Latesha Love-Grayer
OIG - Norman Brown

Department of State Response to GAO Draft Report

CYBERSECURITY: State Needs to Expeditiously Implement Risk Management and Other Key Practices
(GAO-23-107012, GAO Code 107012)

Thank you for the opportunity to comment on the draft report, *Cybersecurity: State Needs to Expeditiously Implement Risk Management and Other Key Practices*.

Recommendation 1: The Secretary of State should direct the CIO to develop and maintain a department-wide risk profile that prioritizes the Department's most significant risks, including eight areas of exposure and threats that State identified consistent with federal requirements.

Department Response: The Department concurs with this recommendation.

Recommendation 2: The Secretary of State should direct the CIO to develop plans to mitigate vulnerabilities in the eight areas of exposure and threats that State previously identified.

Department Response: The Department concurs with this recommendation.

Recommendation 3: The Secretary of State should direct the CIO to conduct bureau-level risk assessments for the 28 bureaus that owned information systems, that we reviewed.

Department Response: The Department concurs with this recommendation.

Recommendation 4: The Secretary of State should direct the CIO to ensure that system security plans for the Comptroller and Global Financial Service Splunk and iPost are updated at least annually, as required by Department policies.

Department Response: The Department concurs with this recommendation.

Recommendation 5: The Secretary of State should direct the CIO to ensure that its information systems have valid authorizations to operate in accordance with Department policies and federal guidance.

Department Response: The Department concurs with this recommendation.

Recommendation 6: The Secretary of State should direct the CIO to assess, prioritize and allocate available Department-wide resources to address the constraints that contribute to the backlog of its assessment and authorization process.

Department Response: The Department concurs with this recommendation.

Recommendation 7: The Secretary of State should direct the CIO to ensure that system owners define and document minimum frequency requirements for continuous monitoring of security controls.

Department Response: The Department concurs with this recommendation.

Recommendation 8: The Secretary of State should direct the CIO to implement all components of its Information Security Continuous Monitoring Program across the Department, including the continuous diagnostic and mitigation capabilities, in accordance with Department policies and federal guidance.

Department Response: The Department concurs with this recommendation.

Recommendation 9: The Secretary of State should ensure the CIO has access to assets at bureaus and posts to continuously monitor for threats and vulnerabilities that may affect mission operations.

Department Response: The Department concurs with this recommendation.

Recommendation 10: The Secretary of State should direct the Assistant Secretary of State for Diplomatic Security to ensure that its incident response procedures are tested annually in accordance with Department policies.

Department Response: The Department concurs with this recommendation.

Pursuant to this recommendation, DS will amend and update the Standard Operating Procedures for the Cyber Incident Response program to fully coordinate existing testing and review processes and establish a formal annual incident response plan testing procedure to include the following provisions:

- Annual review and update of the Significant Cyber Incident Response Plan.
- Annual review of Red Cell test activities to enhance the effectiveness of CIRT program capabilities and procedures.
- Annual review of the continuity of operations exercise to incorporate lessons learned and technology enhancements.

Recommendation 11: The Secretary of State should direct the CIO to annually update the iPost information system contingency plan in accordance with Department policies and federal guidance.

Department Response: The Department concurs with this recommendation.

Recommendation 12: The Secretary of State should direct the CIO to annually test the contingency plan for the Integrated Enterprise Management System in accordance with Department policies.

Department Response: The Department concurs with this recommendation.

Recommendation 13: The Secretary of State should direct the Assistant Secretary of State for Diplomatic Security to ensure that all 30 HVA system contingency plans are tested annually as required by Department policies.

Department Response: The Department concurs with this recommendation.

Recommendation 14: The Secretary of State should direct the CIO to update the October 2020 matrix to better ensure compliance with applicable Department policies and federal guidance. The update could involve operationalizing the matrix describing the roles and responsibilities of the various bureaus so the Department can better address cybersecurity requirements.

Department Response: The Department concurs with this recommendation.

Recommendation 15: The Secretary of State should direct the CIO and the Assistant Secretary for DS to ensure that IRM and DS provide more effective communication about the operation of IT systems to Information System Security Officers at overseas posts regarding Department policies and guidance.

Department Response: The Department concurs with this recommendation.

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Jennifer R. Franks, (404) 679-1831, franksj@gao.gov

Latesha Love-Grayer, (202) 512-4409, lovegrayerl@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Vijay D'Souza (Director); Edward Alexander Jr., Rob Ball, Larry Crosland, Nicole Jarvis, and Duc Ngo (Assistant Directors); Vernetta Y. Marquis (Analyst in Charge); Lauri Barnes, Christopher Businsky, Pamela Davidson, Rebecca Eyler, José Peña III, Zsaroq Powe, Priscilla Smith, and Henry Sutanto made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548