United States Government Accountability Office

Report to Congressional Requesters

July 2019

CYBERSECURITY

Agencies Need to Fully Establish Risk Management Programs and Address Challenges

Accessible Version

GAO-19-384

GAO Highlights

Highlights of GAO-19-384, a report to congressional requesters

July 2019

CYBERSECURITY

Agencies Need to Fully Establish Risk Management Programs and Address Challenges

Why GAO Did This Study

Federal agencies face a growing number of cyber threats to their systems and data. To protect against these threats, federal law and policies emphasize that agencies take a risk-based approach to cybersecurity by effectively identifying, prioritizing, and managing their cyber risks. In addition, OMB and DHS play important roles in overseeing and supporting agencies' cybersecurity risk management efforts.

GAO was asked to review federal agencies' cybersecurity risk management programs. GAO examined (1) the extent to which agencies established key elements of a cybersecurity risk management program; (2) what challenges, if any, agencies identified in developing and implementing cybersecurity risk management programs; and (3) steps OMB and DHS have taken to meet their risk management responsibilities and address any challenges agencies face. To do this, GAO reviewed policies and procedures from 23 civilian *Chief Financial Officers Act of 1990* agencies and compared them to key federal cybersecurity risk management practices, obtained agencies' views on challenges they faced, identified and analyzed actions taken by OMB and DHS to determine whether they address agency challenges, and interviewed responsible agency officials.

What GAO Recommends

GAO is making 57 recommendations to the 23 agencies and one to OMB, in coordination with DHS, to assist agencies in addressing challenges. Seventeen agencies agreed with the recommendations, one partially agreed, and four, including OMB, did not state whether they agreed or disagreed. GAO continues to believe all its recommendations are warranted.

View GAO-19-384. For more information, contact Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

Key practices for establishing an agency-wide cybersecurity risk management program include designating a cybersecurity risk executive, developing a risk management strategy and policies to facilitate risk-based decisions, assessing cyber risks to the agency, and establishing coordination with the agency's enterprise risk management (ERM) program. Although the 23 agencies GAO reviewed almost always designated a risk executive, they often did not fully incorporate other key practices in their programs:

- Twenty-two agencies established the role of cybersecurity risk executive, to provide agency-wide management and oversight of risk management.
- Sixteen agencies have not fully established a cybersecurity risk management strategy to delineate the boundaries for risk-based decisions.
- Seventeen agencies have not fully established agency- and system-level policies for assessing, responding to, and monitoring risk.
- Eleven agencies have not fully established a process for assessing agency-wide cybersecurity risks based on an aggregation of system-level risks.
- Thirteen agencies have not fully established a process for coordinating between their cybersecurity and ERM programs for managing all major risks.

Until they address these practices, agencies will face an increased risk of cyber-based incidents that threaten national security and personal privacy.

Agencies identified multiple challenges in establishing and implementing cybersecurity risk management programs (see table).

Agency Challenges in Establishing Cybersecurity Risk Management Programs

Challenge	Agencies reporting challenge
Hiring and retaining key cybersecurity management personnel	23
Managing competing priorities between operations and cybersecurity	19
Establishing and implementing consistent policies and procedures	18
Establishing and implementing standardized technology capabilities	18
Receiving quality risk data	18
Using federal cybersecurity risk management guidance	16
Developing an agency-wide risk management strategy	15
Incorporating cyber risks into enterprise risk management	14

Source: GAO analysis of agency data. | GAO-19-384

In response to a May 2017 executive order, the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) identified areas for improvement in agencies' capabilities for managing cyber risks. Further, they have initiatives under way that should help address four of the challenges identified by agencies—hiring and retention, standardizing capabilities, receiving quality risk data, and using guidance. However, OMB and DHS did not establish initiatives to address the other challenges on managing conflicting priorities, establishing and implementing consistent policies, developing risk management strategies, and incorporating cyber risks into ERM. Without additional guidance or assistance to mitigate these challenges, agencies will likely continue to be hindered in managing cybersecurity risks.

Contents

Tables

Figures

Abbreviations

Agriculture	U.S. Department of Agriculture
CDM	continuous diagnostics and mitigation
CFO Act	Chief Financial Officers Act
CIO	chief information officer
CISO	chief information security officer
Commerce	Department of Commerce
DHS	Department of Homeland Security
Education	Department of Education
EO	executive order
EPA	Environmental Protection Agency
ERM	enterprise risk management
FISMA	Federal Information Security Modernization Act of 2014
GSA	General Services Administration
HHS	Department of Health and Human Services
HUD	Housing and Urban Development
Interior	Department of the Interior
IT	information technology
Justice	Department of Justice
Labor	Department of Labor
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSF	National Science Foundation

OMB	Office of Management and Budget
OPM	Office of Personnel Management
POA&M	plan of action and milestones
SBA	Small Business Administration
SP	special publication
SSA	Social Security Administration
State	Department of State
Transportation	Department of Transportation
Treasury	Department of the Treasury
USAID	United States Agency for International Development
VA	Department of Veterans Affairs

U.S. GOVERNMENT ACCOUNTABILITY OFFICE

**441 G St. N.W.
Washington, DC 20548**

July 25, 2019

Congressional Requesters

Federal agencies face cyber threats that continue to grow in number and sophistication. Yet, as GAO has previously reported, agencies have struggled to implement programs to effectively manage the risks to their information and information systems.

To protect against cyber threats, agencies must make decisions about how to most effectively secure their systems and data, based on an assessment of the risks they face. The *Federal Information Security Modernization Act of 2014* (FISMA),[1] executive orders, and guidance from the Office of Management and Budget (OMB) explicitly emphasize using risk-based processes for information security. In addition, the National Institute of Standards and Technology (NIST) has developed a framework for managing cybersecurity risk at the agency, business, and system levels.

Executive Order (EO) 13800, issued in May 2017, states that agency heads are to be held accountable for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data.[2] Toward this end, the EO sets forth a number of specific actions to be taken by agencies, OMB, and the Department of Homeland Security (DHS) in order to evaluate and improve cybersecurity risk management across the executive branch.

You asked us to conduct a review of federal agencies' cybersecurity risk management programs. Accordingly, our review examined

[1] The *Federal Information Security Modernization Act of 2014* (FISMA 2014) Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III*, E-Government Act of 2002*, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this report, FISMA refers both to FISMA 2014 and to those provisions of FISMA 2002 that were either incorporated into FISMA 2014 or were unchanged and continue in full force and effect.

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

(1) the extent to which agencies established key elements of a cybersecurity risk management program;

(2) what challenges, if any, agencies identified in developing and implementing cybersecurity risk management programs; and

(3) what steps OMB and DHS have taken to meet their risk management responsibilities under EO 13800 and to address any challenges agencies face in implementing cyber risk management practices.

In conducting this engagement, we focused on the 23 civilian *Chief Financial Officers Act of 1990* (CFO Act) agencies.[3] We excluded the Department of Defense, because the department determined the information we requested pertaining to cybersecurity risk management to be classified and, therefore, not available in a public report.

To address our first objective, we reviewed policies, procedures, and other documentation from the 23 agencies and compared them to selected federal practices identified in OMB and NIST guidance. In selecting the practices for our assessment, we focused on those practices identified by OMB and NIST as foundational for an organization-wide approach to cybersecurity risk management. We also interviewed cognizant agency officials regarding any gaps we identified in agencies' policies and procedures and to understand their approach to cybersecurity risk management.

To address the second objective, we developed and administered structured interview questions to officials responsible for cybersecurity risk management at the 23 agencies to obtain these officials' views on challenges the agencies face in developing and implementing policies

[3] The CFO Act, Pub. L. No. 101-576, 104 Stat. 2838 (Nov. 15, 1990), as amended, established chief financial officers to oversee financial management activities at 23 civilian executive departments and agencies as well as the Department of Defense.

The list now includes 24 entities, which are often referred to collectively as CFO Act agencies, and is codified, as amended, in section 901 (b) of Title 31 of the U.S. Code. The 24 agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

and procedures for managing cybersecurity risk. Specifically, we developed a list of potential challenges based on our assessment of agencies' policies and procedures, a review of OMB's risk report on agencies' cybersecurity risk management capabilities, and reviews of prior GAO reports in areas related to cybersecurity risk management. We asked agency officials to indicate if they experienced these, or any other, challenges in establishing their cybersecurity risk management programs. We also asked them to provide specific examples. We received responses from all 23 agencies. We analyzed the responses to identify those challenges that were identified by a majority of the agencies.

To address the third objective, we reviewed EO 13800 and implementation guidance issued by OMB, as well as relevant reports and other documentation, including OMB's *Federal Cybersecurity Risk Determination Report and Action Plan*, OMB memos, and supporting documentation for DHS initiatives. We also interviewed OMB and DHS officials to gain an understanding of these and other relevant initiatives under way to help agencies implement their cybersecurity risk management programs. We then compared the initiatives to the challenges identified by agencies to determine if they addressed the challenges.

We conducted this performance audit from February 2018 to July 2019 in accordance with generally accepted government auditing standards. 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. A more complete description of our objectives, scope, and methodology is provided in appendix I.

Background

Federal agencies are dependent on information technology (IT) systems and electronic data to carry out operations and to process, maintain, and report essential information. These systems are highly complex and dynamic, technologically diverse, and often geographically dispersed. However, the IT systems supporting federal agencies and our nation's critical infrastructures are at risk.

Information and systems are subject to serious threats that can have adverse impacts on organizational operations and assets, individuals, other organizations, and the nation. These threats can include purposeful attacks, environmental disruptions, and human/machine errors, and may result in harm to the national and economic security interests of the United States.

In recognition of the growing threat, we designated information security as a government-wide high-risk area since 1997. In 2003, we expanded the information security high-risk area to include the protection of critical cyber infrastructure. We further expanded the information security high-risk area in 2015 to include protecting the privacy of personally identifiable information.[4]

Cybersecurity incidents continue to impact federal agencies, as well as entities across various critical infrastructure sectors. In fiscal year 2017, federal executive branch civilian agencies reported 35,277 incidents to the U.S. Computer Emergency Readiness Team. These incidents included web-based attacks, phishing,[5] and the loss or theft of computing equipment. These incidents and others like them can pose a serious challenge to economic and national security and personal privacy. The following examples highlight the impact of such incidents:

- In January 2019, the Department of Justice (Justice) announced that it had indicted two Ukrainian men for their roles in a large-scale, international conspiracy to hack into the Securities and Exchange Commission's computer systems and profit by trading on critical information they stole. The indictment alleges that the two hacked into the Commission's Electronic Data Gathering, Analysis, and Retrieval system and stole thousands of files, including annual and quarterly earnings reports containing confidential, non-public, financial information, which publicly traded companies are required to disclose to the Commission.
- In March 2018, a joint alert from DHS and the Federal Bureau of Investigation stated that Russian government actors had been targeting the systems of multiple U.S. government entities and critical infrastructure sectors since at least March 2016. These Russian

[4] For our most recent update on this high-risk area see GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[5] Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

government actors had affected multiple organizations in various sectors, to include energy, nuclear, water, aviation, construction, and critical manufacturing. DHS and the Federal Bureau of Investigation characterized this activity as a multi-stage intrusion campaign by Russian government cyber actors who targeted small commercial facilities' networks where they staged malware,[6] conducted spear phishing,[7] and gained remote access into energy sector networks.

- In June 2015, the Office of Personnel Management (OPM) reported that an intrusion into its systems had affected the personnel records of about 4.2 million current and former federal employees. Then, in July 2015, the agency reported that a separate, but related, incident had compromised its systems and the files related to background investigations for 21.5 million individuals. In total, OPM estimated 22.1 million individuals had some form of personally identifiable information stolen, with 3.6 million being a victim of both breaches.

The risks to IT systems supporting the federal government and the nation's critical infrastructure are increasing as security threats continue to evolve and become more sophisticated. These risks include insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, steady advances in the sophistication of attack technology, and the emergence of new and more destructive attacks. Therefore, it is imperative for agency leaders and managers at all levels to manage the risks associated with the operation and use of information systems that support their missions and business functions.

Cybersecurity risk management comprises a full range of activities undertaken to protect IT and data from unauthorized access and other cyber threats; maintain awareness of cyber threats; detect anomalies and incidents adversely affecting IT and data; and mitigate the impact of, respond to, and recover from incidents. Information sharing facilitates and supports all of these activities.

[6] Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples include logic bombs, Trojan horses, ransomware, viruses, and worms.

[7] Spear phishing is a form of phishing that uses authentic looking emails, websites, or instant messages that are closely tailored to their intended audience to get users to download malware, open malicious attachments, or open links that direct them to a website that requests information or executes malicious code.

Federal Law and Policy Set Roles and Responsibilities for Protecting Federal Systems and Managing Cybersecurity Risk

Several federal laws, executive orders, and policies establish requirements for protecting federal systems and managing cybersecurity risks. Specifically, FISMA is intended to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, as well as the effective oversight of information security risks. The act requires each agency to develop, document, and implement an agency-wide information security program to provide risk-based protections for the information and information systems that support the operations and assets of the agency, including those provided or managed by another entity.

FISMA also assigns government-wide responsibilities to key agencies:

- OMB is responsible for developing and overseeing implementation of policies, principles, standards, and guidelines on information security in federal agencies, except with regard to national security systems.
- DHS is responsible for certain operational aspects of agencies' information security policies and practices, including assisting OMB in fulfilling its FISMA authorities, issuing binding operational directives, monitoring agencies' security policies and practices, and assisting them with implementation.
- NIST is responsible for developing standards for categorizing information and information systems, security requirements for information and systems, and guidelines for detection and handling of security incidents.

More recently, the administration has re-emphasized the importance of improving agencies' cybersecurity risk management capabilities through the issuance of an executive order. Further, OMB has issued minimum requirements, standards, and guidance to ensure federal managers are effectively managing cybersecurity risks. OMB has also issued policies for enterprise risk management (ERM), which considers all key risks that agencies face and their potential impacts on the agency's mission. Cybersecurity risk is just one type of risk that agencies consider in their enterprise approach to risk management. Table 1 identifies the administration's May 2017 executive order and relevant OMB publications and guidance on cybersecurity risk management.

Table 1: Executive Order and Office of Management and Budget (OMB) Requirements, Standards, and Guidance on Cybersecurity Risk Management

Document Name	Description
Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017)	States that agency heads will be held accountable for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data. It further requires agencies to use the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* to manage their cybersecurity risks and to report to OMB and the Department of Homeland Security (DHS) on their risk mitigation and acceptance choices and plans to implement the framework. The order further requires OMB and DHS to assess each agency's report and to develop a risk determination report for the entire executive branch enterprise.
OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016)	Requires agencies to implement an enterprise risk management (ERM) capability that is coordinated with the strategic planning and strategic review process established by the *GPRA (Government Performance and Results Act) Modernization Act of 2010*, and with the internal control processes required by the *Federal Managers' Financial Integrity Act of* 1982 and in GAO's *Standards for Internal Control in the Federal Government*.[a] This integrated governance structure is designed to improve mission delivery, reduce costs, and focus corrective actions towards key risks. ERM allows management to understand an agency's portfolio of top-risk exposures, which could affect the agency's success in meeting its goals. ERM is part of overall agency governance and accountability functions and encompasses all areas where an organization is exposed to risk (financial, operational, reporting, compliance, governance, strategic, reputation, etc.).
OMB Circular A-130, *Managing Information as a Strategic Resource* (July 2016)	Establishes minimum requirements for federal information security programs, assigns federal agency responsibilities for the security of information and information systems, and links agency information security programs and agency management control systems established in accordance with OMB Circular A-123. It requires agencies to develop and implement an agency-wide risk management process that frames, assesses, responds to, and monitors information security and privacy risk on an ongoing basis across the organization (e.g., agency), mission or business process, and information system level. It also requires agencies to implement a risk management framework to guide and inform the categorization of federal information and information systems; the selection, implementation, and assessment of security and privacy controls; the authorization of information systems and common controls; and the continuous monitoring of information systems.
OMB M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017)	Provides specific guidance to meet the requirements of the Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, including requiring each agency to designate a senior accountable official for risk management; report on the agency's risk management assessment using *Federal Information Security Modernization Act* (FISMA) metrics established by OMB, DHS, and the federal cybersecurity community; and develop an action plan for implementing the NIST cybersecurity framework.
OMB M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements* (October 2018)	Outlines quarterly FISMA reporting requirements, as well as requirements related to various information security and privacy initiatives. These initiatives include identifying federal high-value assets; incident reporting; scanning Internet-accessible addresses and systems; maturing and consolidating agency security operations centers; implementing a cyber threat framework; and implementing DHS's Continuous Diagnostics and Mitigation program.

Source: Executive Order on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* and Office of Management and Budget guidance. | GAO-19-384

[a] GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

In its responsibility for certain operational aspects of agencies' implementation of cybersecurity practices, DHS is spearheading several initiatives to assist federal agencies in protecting their computer networks and electronic information. Examples of DHS's initiatives are described in table 2.

Table 2: Examples of the Department of Homeland Security's (DHS) Cybersecurity Risk Management Initiatives

Initiative	Description
United States Computer Emergency Readiness Team	DHS operates the team, which was established to aggregate and disseminate cybersecurity information to improve warnings and responses to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection.
Continuous Diagnostics and Mitigation (CDM) Program	The program supplies federal agencies with tools and services that are intended to provide them with the capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed into a dashboard that alerts network managers and enables the agency to allocate resources based on the risk.
Federal Information Security Modernization Act (FISMA) Reporting Metrics and Binding Operational Directives	DHS assists the Office of Management and Budget (OMB) in the development of the annual FISMA reporting metrics, which are used by OMB and DHS to compile the annual FISMA report to Congress. Within DHS, the Federal Network Resilience division's Cybersecurity Performance Management Branch is responsible for (1) developing and disseminating FISMA reporting metrics, (2) managing the CyberScope web-based application[a] and (3) collecting and reviewing federal agencies' cybersecurity data submissions and monthly data feeds to CyberScope. Pursuant to FISMA, DHS also develops and oversees the implementation of binding operational directives.[b]

Source: GAO reports on federal information security and OMB guidance. | GAO-19-384

[a] CyberScope is the reporting system managed by the Department of Homeland Security through which agencies are to report their FISMA-related performance metrics.

[b] A binding operational directive is a compulsory direction to federal agencies for purposes of safeguarding federal information and information systems.

NIST Has Established a Framework for Federal Cybersecurity Risk Management Activities

Implementing effective cybersecurity requires any organization—whether a private sector company; a non-profit entity; or an agency at the state, local, or federal level—to identify, prioritize, and manage cyber risks across its enterprise.[8] Risk management is a comprehensive process that requires organizations to (1) frame risk (i.e., establish the context for risk-based decisions), (2) assess risk, (3) respond to risk once determined, and (4) monitor risk on an ongoing basis using effective organizational

[8] OMB, *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018).

communications and a feedback loop for continuous improvement in the risk-related activities of organizations.[9]

In accordance with its responsibilities under FISMA, as well as other laws and executive orders, NIST has developed a framework for managing risk to federal information and information assets. This framework calls for a multi-tiered approach to risk management, with activities at the information system (system),[10] business/mission,[11] and organization[12] (e.g., agency) level. Cybersecurity risk management activities at the organization level provide the foundation for activities at the mission/business process and system levels, such as the selection and implementation of security controls and decisions about the operation of systems based on a determination of risk. Figure 1 illustrates an organization-wide approach to cybersecurity risk management.

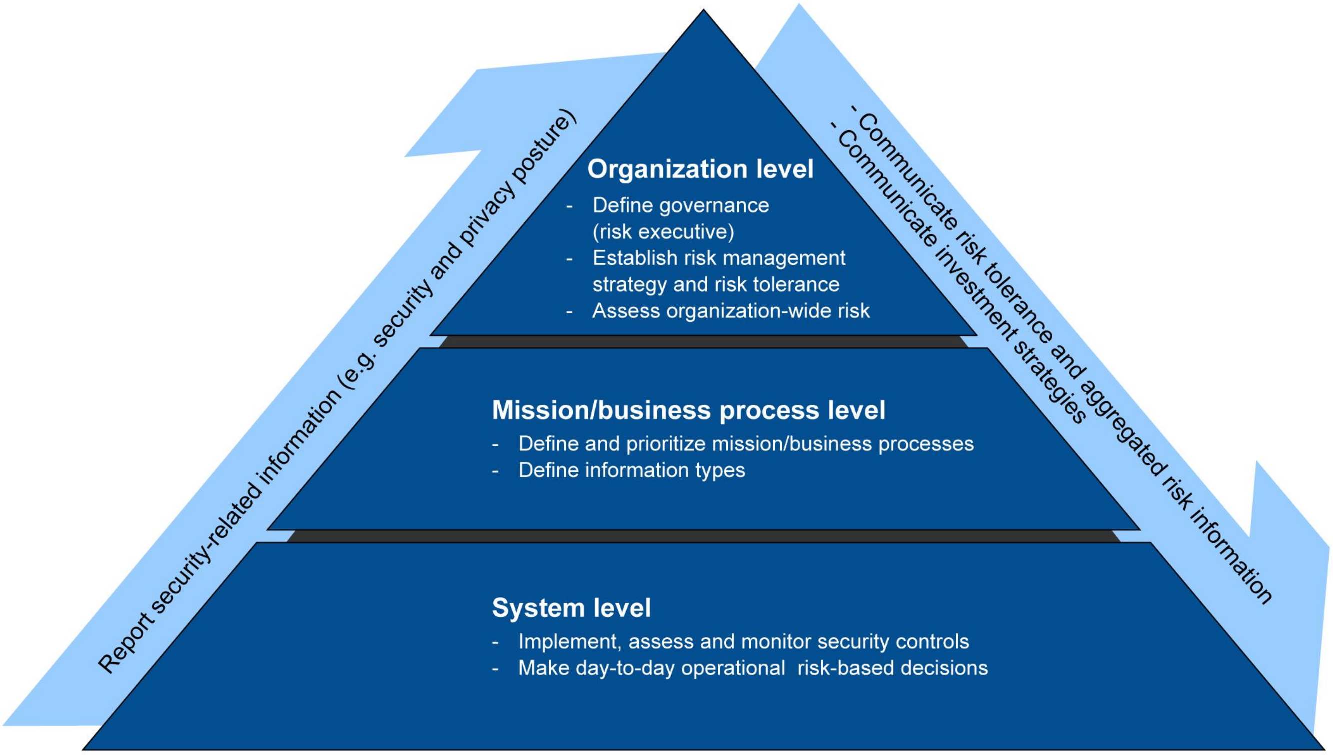
[9] NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* Special Publication (SP) 800-39 (Gaithersburg, Md.: March 2011).

[10] Activities at the *information system level* include categorizing information systems; allocating security controls to these systems; and managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls.

[11] Activities at the *business/mission level* include defining the mission/business processes needed to support the missions and business functions, their information and information flows, and the relevant security requirements.

[12] Activities at the *organization level* include providing the context for all risk management activities carried out by organizations; selecting common controls; the provision of guidance from the risk executive (function) to authorizing officials; and the establishment of the order of recovery for information systems supporting critical missions and business operations.

Figure 1: Organizational Approach to Cybersecurity Risk Management


Report security-related information (e.g. security and privacy posture)
- Communicate risk tolerance and aggregated risk information
- Communicate investment strategies
Organization level
- Define governance (risk executive)
- Establish risk management strategy and risk tolerance
- Assess organization-wide risk
Mission/business process level
- Define and prioritize mission/business processes
- Define information types
System level
- Implement, assess and monitor security controls
- Make day-to-day operational risk-based decisions

Source: GAO based on National Institute of Standards and Technology Special Publications 800-39,800-37, and NISTIR 8170. | GAO-19-384

Guidance for federal agencies' cybersecurity risk management processes is found in a suite of NIST special publications. Table 3 highlights key NIST cybersecurity risk management publications.

Table 3: Key National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Publications

Publication	Description
Framework for Improving Critical Infrastructure Cybersecurity, v. 1.1	Provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. The framework is a set of cybersecurity activities, outcomes, and informative references that are common across sectors and provide guidance for developing individual organization profiles. The framework consists of five concurrent and continuous functions—identify, protect, detect, respond, and recover. When considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk. While the framework was originally developed for use by critical infrastructure sectors, Executive Order 13800 requires federal agencies to use it to manage their cybersecurity risks. The framework can be used with a broad array of cybersecurity risk management processes, including those developed by NIST for use by federal agencies. In May 2017, NIST issued a draft publication for public comment (NISTIR 8170) that is intended to provide federal agencies with guidance

Publication	Description
	on implementing the framework.
Special Publication 800-30: *Guide for Conducting Risk Assessments* (September 2012)	Provides guidance for conducting risk assessments, amplifying the guidance in NIST Special Publication 800-39 (discussed later in this table). In particular, it includes guidance on carrying out a risk assessment process and on how risk assessments and other risk management processes complement and inform each other.
Special Publication 800-37, Revision 1: *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010, updated June 2014)	Explained how to apply the risk management framework to federal information systems, including security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring. This publication is to be officially withdrawn on December 20, 2019.
Special Publication 800-37, Revision 2: *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (December 2018)	Supersedes revision 1 and provides updated guidance for implementing NIST's risk management framework for information systems. Among other things, the revision includes activities organized under an additional "prepare" step in NIST's risk management framework. NIST notes that the activities organized under the "prepare" step are not new, but have been included in existing NIST guidance. The purpose of this step is to carry out essential activities at the organization, mission and business process, and system levels of the organization to establish the context and help prepare the organization to manage its security and privacy risks. These include, among other things, assigning key roles and responsibilities for executing the risk management framework; establishing a risk management strategy and organizational risk tolerance; conducting risk assessments; identifying, documenting, and publishing common controls that are available for inheritance by organizational systems; and developing an organization-wide strategy for monitoring control effectiveness.
Special Publication 800-39: *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011)	Provides guidance for an integrated, organization-wide program for managing information security risk. It provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.
Special Publication 800-53, Revision 4: *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013)	Provides a catalog of security and privacy controls for federal information systems and agencies. It also provides a process for selecting controls to protect agency operations, assets, individuals, and the nation from a diverse set of threats. These threats include hostile cyber attacks, natural disasters, structural failures, and human errors.

Source: NIST. | GAO-19-384

Federal Guidance Includes Key Steps for Establishing Cybersecurity Risk Management Programs

OMB and NIST guidance identify practices for establishing agency-wide cybersecurity risk management programs.[13] Among other things, these

[13] NIST Special Publication (SP) 800-39 defines an organization as an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements) that is charged with carrying out assigned mission/business processes and that uses information systems in support of those processes. Throughout this report, we refer to organization-level activities as *agency-level* or *agency-wide* activities.

activities are intended to facilitate better communication between senior leaders and executives and system owners and operators; align agency priorities with resource allocation and prioritization at the system level; and convey acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance. Practices that provide a foundation for an agency's cybersecurity risk management program are summarized in table 4.

Table 4: Foundational Practices for Establishing Cybersecurity Risk Management Programs

Practice	Description
Establish the role of a cybersecurity risk executive	Agencies should assign an individual or group that provides agency-wide oversight of cybersecurity risk activities and facilitates collaboration among stakeholders and consistent application of the cybersecurity risk management strategy.
Develop a cybersecurity risk management strategy	Agencies should establish a strategy to develop a foundation for managing cybersecurity risk and delineate the boundaries for risk-based decisions, which should inform how security and privacy risk is framed, assessed, responded to, and monitored.
Document risk-based policies	Agencies should document agency-wide policies and procedures that include key elements to facilitate risk-based decision making in managing cybersecurity risks.
Conduct an agency-wide cybersecurity risk assessment	Agencies should assess organization-wide cybersecurity risk based primarily on aggregated information from system-level risk assessments, continuous monitoring, and any relevant strategic risk considerations. The assessment is to allow the organization to consider the totality of risk derived from the operation and use of its information systems.
Establish coordination between cybersecurity and enterprise risk management	Agencies should account for information security risk when making operational decisions with regard to their mission/business processes and ensure that cybersecurity risk information is shared with key stakeholders throughout the organization.

Source: GAO analysis based on OMB and NIST guidance. | GAO-19-384

Establish the role of a cybersecurity risk executive: In order to ensure that cybersecurity risks are being addressed across the agency, NIST Special Publication 800-39 states that agencies should establish a cybersecurity risk executive. This can take the form of an individual or group that provides agency-wide oversight of cybersecurity risk activities and facilitates collaboration among stakeholders and consistent application of the cybersecurity risk management strategy. The cybersecurity risk executive should ensure that risk-related considerations for information systems are viewed from an agency-wide perspective regarding the strategic goals and objectives. The cybersecurity risk executive also should ensure that cybersecurity risk is managed consistently across the agency, reflects organizational risk tolerance, and is considered along with other types of risk to ensure mission/business success.

Develop a cybersecurity risk management strategy: According to NIST Special Publication 800-39 and other guidance,[14] agencies should develop a cybersecurity risk management strategy to provide a foundation for managing risk and delineate the boundaries for risk-based decisions. The strategy should describe the strategic-level decisions and considerations that senior leaders and executives are to use to manage security and privacy risks to agency operations, assets, individuals, other organizations, and the nation. The strategy should also guide and inform how security and privacy risks are framed, assessed, responded to, and monitored. The strategy should include (1) a statement of the agency's risk tolerance,[15] (2) how it intends to assess risk (e.g., acceptable risk assessment methodologies), (3) acceptable risk response strategies (e.g., acceptance, mitigation, avoidance), and (4) how the agency intends to monitor risk over time.

Document risk-based policies: NIST Special Publication 800-37 identifies foundational activities at the agency and information system levels that should be included in policies to help prepare agencies to manage security and privacy risks.[16] These activities should be guided by risk-based decisions. Specific elements of such risk-based policies include (1) identifying and assigning individuals with key roles for executing the risk management framework; (2) requiring an agency-wide assessment of cyber risks; (3) identifying and documenting common security controls that can be inherited by multiple information systems; (4) developing an agency-wide strategy for monitoring control effectiveness; (5) requiring system-level risk assessments to be performed and regularly updated; (6) tailoring system security controls based on risk; (7) prioritizing remedial actions to correct vulnerabilities identified in plans of action and milestones (POA&M) based on risk; and (8) using a determination of risk to make decisions about system operation and use.

[14] See, for example, NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v. 1.1 (April 2018) and *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Rev. 2 (December 2018).

[15] Risk tolerance is the level of risk an entity is willing to assume in order to achieve a potential desired result.

[16] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, SP 800-37, rev. 1 (February 2010, updated June 2014); SP 800-37, rev. 2.

Conduct an agency-wide cybersecurity risk assessment: According to NIST Special Publications 800-39 and 800-37, agencies should assess cybersecurity and privacy risks and update the results on an ongoing basis. Risk assessment at the agency level is based primarily on aggregated information from system-level risk assessment results, continuous monitoring, and any relevant strategic risk considerations. The assessment is intended to help the agency consider the totality of risk derived from the operation and use of its information systems and from information exchanges and connections with other internally and externally owned systems. Such assessments may identify systemic weaknesses or deficiencies discovered in multiple information systems and assess the overall risks that these present to operations, assets, and individuals.

Establish coordination between cybersecurity and enterprise risk management: ERM, as a discipline, deals with identifying, assessing, and managing risks. OMB has stated that an effective enterprise risk management program should promote a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include strategic, market, cyber, legal, reputational, political, and a broad range of operational risks.[17]

Toward this end, OMB Circular A-123 directs agencies to implement a capability for enterprise risk management. Specifically, it encourages agencies to establish a risk management governance structure, such as a risk management council, which may be integrated with existing management structures; develop "risk profiles" that identify risks arising from mission and mission-support operations; and consider those risks as part of the annual strategic review process.

Because cybersecurity is a key risk facing virtually every federal agency, it is important for coordination to exist between agencies' ERM functions and their cybersecurity risk management programs, particularly the cybersecurity risk executive. NIST SP 800-39 states that effective risk management requires an agency's mission/business processes to explicitly account for information security risk when making operational decisions and that cybersecurity risk information should be shared with

[17] OMB, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, M-17-25 (May 2017).

key stakeholders throughout the organization. According to NIST, the risk executive should serve as a common risk management resource for senior leaders, mission/business owners, and other organization officials and as a focal point for communicating and sharing information security risk-related information among key stakeholders.[18] OMB has also raised concerns that agencies' ERM programs do not effectively identify, assess, and prioritize actions to mitigate cybersecurity risks in the context of other enterprise risks.[19] GAO has also emphasized the importance of sharing risk information with stakeholders as part of an effective risk management program.[20]

Agencies Have Not Fully Established Elements of Their Cybersecurity Risk Management Programs

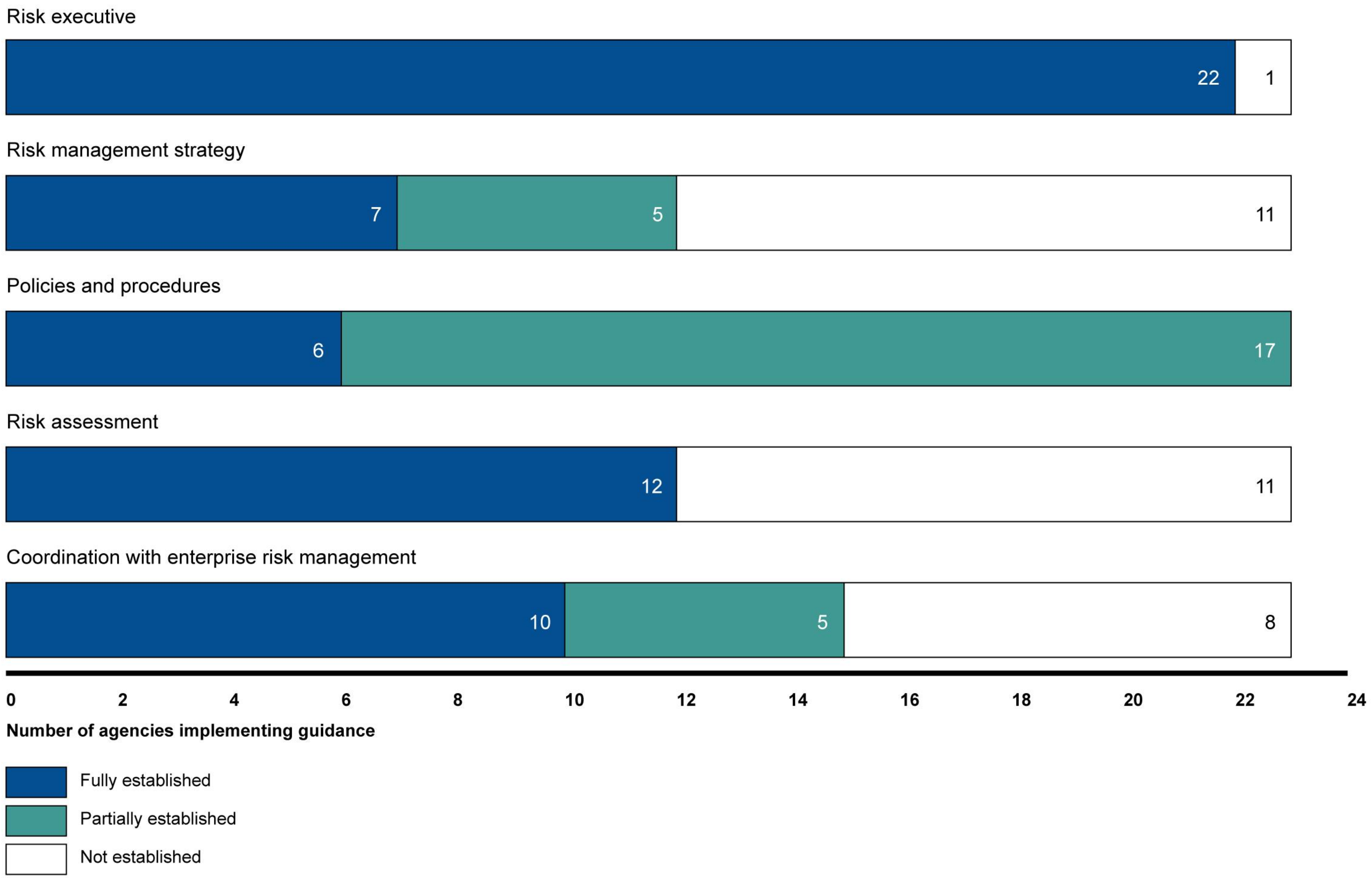
The 23 civilian CFO Act agencies varied in the extent to which they had established key elements of their cybersecurity risk management programs. Specifically, 22 of the 23 agencies established the role of cybersecurity risk executive, and most of the 23 agencies had established policies that include elements to ensure their activities are guided by risk-based decisions. However, fewer than half of the agencies developed an agency-wide cybersecurity risk management strategy or fully established coordination with their enterprise risk management function. Figure 2 summarizes the extent to which the agencies had established these elements as of April 2019.

[18] NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (March 2011).

[19] OMB, *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018).

[20] GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, GAO-17-63 (Washington, D.C.: Dec. 1, 2016).

Figure 2: Extent to Which Agencies Had Established Key Cybersecurity Risk Management Program Elements



Source: GAO analysis of agency data. | GAO-19-384

Most Agencies Established the Role of Cybersecurity Risk Executive

Twenty-two of the 23 civilian CFO Act agencies established a cybersecurity risk executive to provide agency-wide oversight of cybersecurity risk activities. Agencies varied in assigning this responsibility to the chief information officer (CIO), chief information security officer (CISO), or another official or entity. For example:

- At the Department of Health and Human Services (HHS), the CIO serves as the risk executive for the department, and is responsible for executing the Risk Management Framework tasks outlined in NIST SP 800-37.

- The United States Agency for International Development (USAID) designated the CISO with responsibility for carrying out the risk executive functions for the agency. Among other things, the CISO is responsible for developing, implementing, and managing an agency-wide security authorization process and a threat awareness program.
- The Department of the Treasury (Treasury) assigned the function of risk executive to its department CIO Council. The council's responsibilities include ensuring the cybersecurity program is consistent with the provisions of NIST SP 800-39; providing guidance to and oversight of the organization's risk management program and developing the cybersecurity risk management strategy; communicating organization-wide threat, vulnerability, and risk-related information; and providing a strategic view for managing cyber risk throughout the organization.

One agency, the General Services Administration (GSA), had not defined the role of its cybersecurity risk executive in its policy. Officials in GSA's Office of the CIO stated that they had not formally designated this role because the agency's risk executive responsibilities were shared among the CIO, CISO, authorizing officials, and other GSA officials for risk management. However, without clearly defining and documenting the responsibility for the risk executive function, the agency may lack consistent implementation and oversight of cybersecurity risk management activities and an effective agency-wide view for managing risk. Additional details on the 23 agencies' cyber risk executive positions are provided in appendix II.

Most Agencies Did Not Develop an Agency-Wide Cybersecurity Risk Management Strategy to Guide Their Risk Decisions

Among the 23 civilian CFO Act agencies, seven had developed a cybersecurity risk management strategy that fully addressed the four elements called for in the NIST guidance. Specifically, each of the seven agencies (the Department of Commerce (Commerce), the Department of Labor (Labor), the Department of State (State), USAID, GSA, OPM, and the Social Security Administration (SSA)) had developed a strategy to guide how cybersecurity risk is to be framed, assessed, responded to, and monitored. For example, some of the strategies discussed risk tolerance in terms of thresholds based on essential mission functions and the processing of personally identifiable information or system impact levels, types of data processed, and accessibility of systems, among other factors. The strategies also included breakdowns of appropriate risk response strategies and how the agencies intended to assess and monitor risk.

In addition, five of the 23 agencies (the Department of Education (Education), Environmental Protection Agency (EPA), National Science Foundation (NSF), the Department of Transportation (Transportation), and the Small Business Administration (SBA)) had partially developed cybersecurity risk management strategies, but their strategies did not address certain required elements. Specifically, while these agencies developed strategic documents, these documents did not include all of the required elements, such as a statement of risk tolerance or acceptable risk mitigation strategies.

EPA officials stated that they intended to update their strategy documents to address how the agency intends to assess risk, while Education and NSF officials did not state whether they intended to update their strategy to include a statement of risk tolerance, among other missing elements. Transportation and SBA officials stated that they believed their existing strategy documents addressed all the elements; however, neither agency's strategy included an expression of departmental risk tolerance and risk mitigation strategies. Further, Transportation's strategy did not include a description of acceptable risk assessment methodologies.

The remaining 11 agencies had not developed an agency-wide cybersecurity risk management strategy. These agencies offered a variety of reasons for not doing so.

- Seven agencies—the Department of Agriculture (Agriculture), Department of Energy (Energy), HHS, Department of the Interior (Interior), Treasury, the National Aeronautics and Space Administration (NASA), and the Nuclear Regulatory Commission (NRC)—acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. According to agency officials, this was due to the federated nature of the agency or difficulty in establishing an agency-wide understanding of risk tolerance, among other factors. Further, these agencies stated that they intended to develop such a strategy or were considering doing so.
- The other four agencies—DHS, the Department of Housing and Urban Development (HUD), Department of Justice (Justice), and

Department of Veterans Affairs (VA)—stated that they believed their existing documents and policies constituted a risk management strategy. However, we determined that these documents did not constitute an integrated strategy that addressed key elements such as risk tolerance and risk mitigation strategies.

Without a comprehensive risk management strategy, the agencies may lack an organization-wide understanding of acceptable risk levels and appropriate risk response strategies to protect their systems and data. Additional details regarding the 23 agencies' establishment of cybersecurity risk management strategies are discussed in appendix III.

Agencies Established Policies for Implementing Risk Management Activities, but Gaps Remain in Some Areas

Most of the 23 agencies had established policies that include elements to ensure their activities are guided by risk-based decisions. However, many agencies had gaps in one or more of these areas. Specifically, six agencies (DHS, Education, Justice, Treasury, NSF, and SSA) addressed all of these areas in their policies and procedures, while the remaining 17 agencies had not addressed at least one area. Table 5 discusses, for each of these elements, which of the 23 agencies had addressed it in their policies.

Table 5: Extent to Which the 23 Civilian Chief Financial Officer Act Agencies Addressed Key Risk Management Elements in Policies

Policy element	GAO assessment
Identify and assign individuals to specific roles for executing the risk management framework.	All 23 agencies established roles and responsibilities for executing the risk management framework.
An organization-wide risk assessment is completed or an existing risk assessment is updated.	Nine agencies required in their policies that an agency-wide assessment of cyber risks be conducted and updated. The remaining 14 agencies (the Departments of Commerce, Energy, Health and Human Services (HHS), Interior, State, Transportation, and Veterans Affairs (VA); the U.S. Agency for International Development (USAID); Environmental Protection Agency (EPA); General Services Administration (GSA); National Aeronautics and Space Administration (NASA); Nuclear Regulatory Commission (NRC); Office of Personnel Management (OPM); and Small Business Administration (SBA)) did not address this in policy.
Common controls that are available for inheritance by multiple information systems are identified, documented, and published. Common controls are controls that can be inherited by one or more information systems.	Twenty-two agencies had policies for identifying and documenting common controls. One agency—Energy—did not include this in its policy.

Policy element	GAO assessment
An agency-wide strategy for monitoring control effectiveness is developed and implemented. The continuous monitoring strategy identifies the minimum monitoring frequency for implemented controls across the organization; defines the ongoing control assessment approach; and describes how ongoing assessments are to be conducted.	Twenty-two agencies establish a strategy for monitoring control effectiveness on an ongoing basis. However, one agency (State) did not address this in policy.
System-level risk assessments are conducted and updated on an ongoing basis. Assessment of security risk includes identification of threat sources and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets.	Twenty-two agencies had policies that required risk assessments to be conducted for their systems and updated on a regular basis. One agency (State) did not provide such a policy.
When selecting security controls, organizations use risk assessments to inform and guide the tailoring process for organizational information systems and environments of operation.	Seventeen agencies had policies that required the tailoring of security controls to be informed by an assessment of risk. However, six agencies (Agriculture, HHS, Labor, State, USAID, and OPM) did not address this element in their policies.
Risk assessments should inform and guide plan of action and milestones (POA&M) prioritization. Organizations implement a consistent process for developing plans of action and milestones that uses a prioritized approach to risk mitigation that is uniform across the organization. A risk assessment guides the prioritization process for items included in the plan of action and milestones.	Fifteen agencies had policies that called for the prioritization of POA&Ms based on considerations of their risk. However, eight agencies (Agriculture, Commerce, HUD, Labor, State, NASA, NRC, and SBA) did not include this in their policies.
Risk determinations should inform and guide decisions about the operation and use of systems. The authorizing official or designated representative, in collaboration with other security and privacy officials, analyzes the information in the authorization package provided by the control assessor, system owner, or common control provider, and finalizes the determination of risk.	All 23 agencies required determinations of risk to inform decisions about the operation and use of systems.

Source: GAO analysis of agency policies and procedures. | GAO-19-384

Eleven agencies—Agriculture, Commerce, Energy, HHS, Interior, Labor, EPA, GSA, NASA, NRC, and OPM—generally agreed that their policies lacked identified elements and either stated that they intended to update policies to include them or would consider doing so.

The remaining six agencies—HUD, State, Transportation, VA, USAID, and SBA—stated that they believed their policies addressed these elements or that they carried out these activities in practice, but did not provide documentation of policies that addressed them.

Without ensuring that their policies include all key risk management activities, the agencies may not be taking the foundational steps needed to effectively identify and prioritize activities to mitigate cybersecurity risks that could result in the loss of sensitive data or compromise of agency systems. Additional details on the agencies’ risk management policies are provided in appendix IV.

About Half of the Agencies Developed an Agency-Wide Cybersecurity Risk Assessment Process

Twelve of the 23 civilian CFO Act agencies had developed a process or mechanism for conducting an agency-wide cybersecurity risk assessment. Specifically, these agencies (Agriculture, Education, Energy, DHS, HUD, Interior, Justice, Labor, State, Transportation, NSF, and SSA) had developed processes for aggregating system-level data and analyzing them to assess overall cybersecurity risk to agency operations and assets. For example, these 12 agencies developed scorecards or dashboards that provided agency-wide views of key indicators aggregated from system-level information and risk scores for agency components. Officials from seven of these agencies described how these assessments enable them to make enterprise-wide decisions on prioritizing and remediating risks.

The remaining 11 agencies (Commerce, GSA, HHS, NASA, NRC, Treasury, VA, EPA, OPM, SBA, and USAID) offered a variety of reasons for why they did not develop a process for assessing cybersecurity risks at the agency level. Five agencies stated that they were still working to develop or acquire tools that will allow them to aggregate system-level data, and three of these noted that they expected further implementation of DHS's CDM initiative to provide this capability. The other six agencies stated that they did conduct such an assessment in practice, but did not provide sufficient documentation of the process they use.

Without a means of aggregating and assessing cybersecurity risks arising from their information systems to the organizational level, these 11 agencies may be missing opportunities to identify trends or prioritize investments in cybersecurity risk mitigation activities in order to target widespread or systemic risks to the systems and organization. Additional details of agencies' processes for conducting organization-wide cyber risk assessments are contained in appendix V.

Most Agencies Did Not Fully Establish Their Approach to Coordinating between Cybersecurity and Enterprise Risk Management

Ten of the 23 civilian CFO Act agencies provided evidence of having a fully established process for coordination between their cybersecurity risk executive and the entity responsible for overall ERM functions. Five agencies provided evidence of a partially established process, and eight could not provide evidence of such a process.

The ten agencies with fully established processes included this coordination as part of their defined and documented ERM governance structure and process.[21] The agencies took steps to ensure such coordination in a variety of ways. For example, eight agencies, including Education and USAID, established a specific body, such as a risk management council, with responsibility for ERM. These agencies included their cybersecurity risk executive in the council's membership in order to facilitate coordination. Other agencies, such as the National Science Foundation, ensured coordination through regular reporting or briefings between their cybersecurity risk executive and their ERM governance structure.

In addition, five agencies partially established an approach to coordination in this area. These agencies provided some evidence of coordination activities, but had not formally defined or documented this coordination as part of their ERM structure or process. Specifically, four of these agencies (Justice, the Department of Transportation (Transportation), the Environmental Protection Agency (EPA), and the Social Security Administration (SSA)), provided evidence of occasional coordination between their cybersecurity risk executive and officials responsible for ERM. However, they did not fully define and document their ERM governance structures and processes, including how coordination with the cybersecurity risk executive was to take place.

One agency—GSA—had not formally documented the position or responsibilities of the cybersecurity risk executive in its policy. Thus, the agency could not show that the risk executive was involved in ERM activities, although the agency board responsible for ERM does include the agency CIO as a co-chair.

Although they did not provide evidence of a fully documented process, officials from these five agencies stated that they perform this coordination in practice. However, documenting these processes would

[21] These agencies were the Departments of Commerce, Education, Energy, Housing and Urban Development, Labor, National Aeronautics and Space Administration, National Science Foundation, Officer of Personnel Management, Small Business Administration, and U.S. Agency for International Development.

help ensure a consistent, rather than ad-hoc, approach to communication and coordination.

Lastly, eight agencies had not established an approach to coordination in this area. In particular, these agencies (Agriculture, HHS, Interior, VA, DHS, State, Treasury, and NRC) either did not have an ERM governance structure and/or did not provide evidence of a process for coordination between their ERM governance structure and their cybersecurity risk executive.

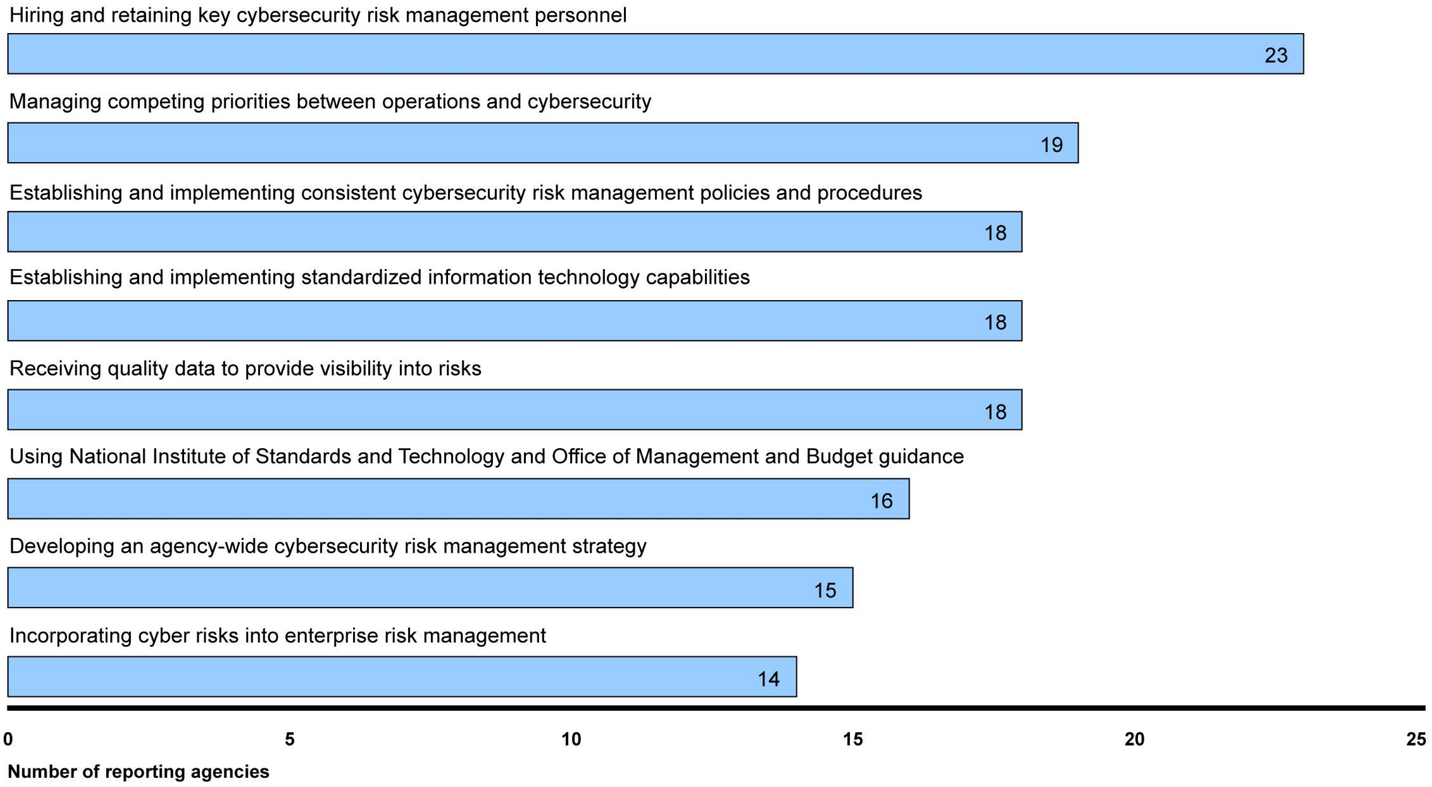
Officials from two of these agencies stated that they were still in the process of formalizing their approach to ERM, while the other six stated that such coordination occurs, even if processes may not be fully documented. However, as noted previously, documenting these processes would help ensure a consistent, rather than ad-hoc, approach to communication and coordination.

Without regular coordination between the cybersecurity risk executive and broader ERM entity, senior leadership responsible for ERM may not be fully aware of significant cybersecurity risks and, thus, may not be positioned to address them in the context of other risks and their potential impacts on the mission of the agency. Additional details on agencies' coordination processes are provided in appendix VI.

Agencies Identified a Variety of Challenges in Developing and Implementing Cybersecurity Risk Management Programs

Officials responsible for cybersecurity risk management at a majority of the 23 civilian CFO Act agencies reported eight challenges in establishing and implementing cybersecurity risk management programs. Most commonly cited were challenges related to hiring and retaining qualified personnel, competing priorities between cybersecurity and agency mission or operations, and establishing and implementing consistent cybersecurity risk management policies and procedures. Figure 3 shows the challenges identified and the number of agencies reporting each challenge.

Figure 3: Challenges Identified by 23 Civilian Chief Financial Officers Act Agencies in Developing and Implementing Cybersecurity Risk Management Programs



Source: GAO analysis of agency data. | GAO-19-384

Hiring and Retaining Key Cybersecurity Risk Management Personnel

All of the 23 civilian CFO Act agencies reported hiring and retaining personnel to fill key cybersecurity risk management positions as a challenge in establishing a cybersecurity risk management program. In particular, six agencies cited the lengthy federal hiring process, and 14 noted the difficulty in competing with private-sector companies in salary and other benefits. Further, 11 agencies noted that there is a shortfall in candidates with the skills needed for cybersecurity risk management. For example:

- NASA's Chief Cyber Risk Officer noted that cybersecurity risk management is a multi-disciplinary field that blends technical cyber expertise with project management principles and a business-focused management background. This official stated that it is difficult to find talent that possesses this multi-disciplinary experience, in part, because current government marketing for cybersecurity skill sets advertise for purely technical skills. The official added that, currently, the government lacks clearly defined roles for cyber risk management as a dedicated job function.

- HUD's CIO saw this challenge as part of a larger shortfall of this highly in-demand resource and noted that HUD must compete with tech giants and Silicon Valley startups for qualified personnel. The official stated that the executive order providing direct hiring authorities for cybersecurity positions provides assistance, though the department still needs to be creative in enhancing retention and recruitment efforts through bonuses and other incentives.

A key to having a successful cybersecurity program is having a well-trained, highly qualified workforce that is versed in identifying cyber threats and recognizes steps to take once confronted with them. Our work has identified difficulties in recruiting and retaining qualified cybersecurity professionals as a continuing challenge.[22] If agencies are unable to hire and retain qualified cybersecurity risk management personnel, they will be hindered in establishing effective programs for cybersecurity risk management.

Managing Competing Priorities between Operations and Cybersecurity

Nineteen of the 23 civilian CFO Act agencies reported competing priorities between agency mission operations and cybersecurity as a challenge. In particular, 12 agencies noted that cybersecurity requirements are sometimes perceived as impeding mission activities, such as deploying systems, sharing information, or providing public services. In addition, four agencies highlighted the competition for limited resources between cybersecurity risk management activities and operational or mission needs. For example:

[22] GAO, *Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions*, GAO-18-466 (Washington, D.C.: June 14, 2018) and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Sept. 6, 2018).

- HHS's Acting Deputy CISO stated that, due to the federated nature of the agency and the broad spectrum of its missions and business functions, there is often a disconnect between security and operational personnel. As an example, the official stated that Operating Divisions that are research or academics focused will require increased information sharing and flexibility, but this often conflicts with cybersecurity concepts and processes.
- Interior's Deputy CIO stated that the need to balance mission priorities with those related to cybersecurity risk management leads to fiscal and operational challenges when making investment, architectural, and operational decisions.

NIST emphasizes determining the relative importance of the mission/business functions in order to make the appropriate level of risk management investment.[23] If agencies are unable to establish priorities among cybersecurity and operational needs, they may be challenged in allocating resources appropriately to ensure their systems and information are appropriately secured.

Establishing and Implementing Consistent Cybersecurity Risk Management Policies and Procedures

Eighteen of the 23 civilian CFO Act agencies reported challenges in establishing and implementing consistent cybersecurity risk management policies and procedures across the organization. Eight agencies cited challenges in this area arising from the difficulty in ensuring consistency across a federated or decentralized organization, while other factors included training staff and making them aware of policies, and the need to integrate cybersecurity policies with missions and operations. For example:

- EPA's CISO related that challenges in consistent implementation of policies and procedures include the need to train individuals involved in the risk management process, address different views of risk appetite within the agency, and deal with varying perspectives on the importance of cybersecurity, among other things.
- OPM's Deputy CISO highlighted that frequent changes in the agency's leadership (e.g., having eight CIOs since 2012) had led to challenges with the agency's ability to implement consistent policies in

[23] NIST SP 800-39.

an ongoing, streamlined manner. As we have previously reported, CIOs and former agency IT executives believed it was necessary for a CIO to stay in office for 3 to 5 years to be effective and 5 to 7 years to fully implement major change initiatives in large public sector organizations.[24] In addition, the Deputy CISO stated that the establishment and implementation of cybersecurity risk management policies and procedures has been viewed as a secondary responsibility, to be accomplished when more pressing and immediate operational concerns do not need attention.

NIST has emphasized the importance of a consistent approach in order for cybersecurity risk management to succeed at all levels of an agency.[25] If agencies are unable to establish consistent cybersecurity risk management policies and procedures, they may not be able to effectively prioritize and implement security and privacy activities to protect their most critical assets and systems.

Establishing and Implementing Standardized IT Capabilities

Eighteen of the 23 civilian CFO Act agencies reported challenges in establishing and implementing standardized IT capabilities across the organization. Eleven of these agencies noted that decentralized or federated organizations create difficulty in implementing standardized, agency-wide tools and solutions to manage cybersecurity risks. In addition, four agencies cited issues with legacy systems, which may not always be compatible with capabilities intended to be used agency wide. For example:

- The Department of Commerce's (Commerce) Deputy CISO stated that, because Commerce is a largely federated agency, with each bureau operating and maintaining its own environment, managing a truly enterprise solution is challenging in numerous areas. For example, the official stated that the department cannot control access at bureaus due to disconnected networks, different security offices and policies, and even different logical access policies. The official added that a change in governance and thinking toward common

[24] GAO, *Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges*, GAO-04-823 (Washington, D.C.: July 21, 2004).

[25] NIST SP 800-37.

enterprise tools and solutions requires a shift in management and thinking across the department and its bureaus.

- Energy's Acting Deputy CIO for Cybersecurity stated that the department is working, to the degree possible, to implement enterprise solutions for cybersecurity and continuous monitoring; however, because the enterprise is comprised of laboratories and sites with very diverse mission sets, doing so is always challenging. This official added that the department has embraced the DHS CDM initiative, which will be leveraged to standardize some IT cybersecurity capabilities, but it does not have a single standardized solution across the enterprise.

OMB recently noted that an agency's ability to mitigate security vulnerabilities becomes more complex in federated agencies, where there are not standardized procedures or technology across the organization.[26] The challenges in implementing standardized IT capabilities may hinder these agencies in applying a consistent level of protection to their systems and data.

Receiving Quality Data to Provide Visibility into Risks

Eighteen of the 23 civilian CFO Act agencies reported that they had experienced challenges in receiving quality data (e.g., accurate, timely information on threats and vulnerabilities). Twelve of these agencies expressed challenges in receiving data from all parts of their agencies or stated that they relied on manual reporting from their components, which did not provide real-time visibility into risks. In addition, six agencies cited difficulties in combining data from disparate sources into an agency-wide view of risk. For example:

- DHS's Acting Director of Governance and Executive Management noted that the department's management currently depends on its components to submit timely and accurate information on cybersecurity vulnerabilities instead of having real-time, centralized reporting of data. The official added that DHS expects to address this challenge through implementation of CDM centralized reporting to the DHS Dashboard on a near real-time basis and other tools and processes for enterprise data collection.

[26] OMB, *Federal Cybersecurity Risk Determination Report and Action Plan* (Washington, D.C.: May 2019).

- State's Enterprise Risk Officer for Cybersecurity reported that threat information is difficult to gather with the specificity needed to make strategic decisions. The official added that, with regard to vulnerability data, sufficient data exist and are gathered on a regular basis; however, it is difficult in a large global enterprise to prioritize actions without credible information on the likelihood of a threat or its impact on the agency's mission.

NIST emphasizes that risk monitoring tools, techniques, and procedures can increase risk awareness and help senior leaders develop a better understanding of the ongoing risk to organizational operations and assets.[27] If the agencies are unable to consistently receive quality, timely data from their entire organizations, they will continue to be challenged in making effective decisions to address organization-wide cybersecurity risks.

Using NIST and OMB Guidance

Sixteen of 23 civilian CFO Act agencies reported the lack of sufficiency, clarity, or usefulness of NIST and/or OMB guidance for cybersecurity risk management as a challenge. Six agencies stated that there was a lack of practical instruction to assist agencies in implementing guidance. Six agencies also stated that various guidance documents are not always consistent or easy to understand. Six agencies also expressed a need for guidance to address new technologies or emerging areas such as the use of cloud providers or establishing cybersecurity risk management programs at all levels of an organization. For example:

- HHS's Acting Deputy CISO stated that, for all the positive aspects of the NIST guidance, there is a lack of a centralized document or road map that ties all the documents together from a cybersecurity standpoint. Also, the official stated that the guidance from NIST provides limited direction for producing specific metrics and checklists in support of laws, policies, directives, instructions, and standards.
- Transportation's CISO stated that current guidance does not always provide agencies with practical ways to implement requirements. For example, the official noted that current OMB guidance on cyber and privacy risk management does not tell agencies how to practically integrate these disciplines, and that frequent updates to NIST guidance that agencies have to respond to might be better applied to

[27] NIST SP 800-39.

identifying practical implementations. The official added that a lack of practical implementation guidance may lead to duplication of effort and inconsistency of outcomes.

OMB and NIST play important roles in issuing policies, standards, and guidelines for agencies' cybersecurity risk management programs. However, if agencies find guidance unclear or insufficient, they will be challenged in implementing key cybersecurity risk management requirements.

Developing a Strategy to Manage Cybersecurity Risks

Fifteen of the 23 CFO Act agencies reported challenges in developing an agency-wide cybersecurity risk management strategy that includes a statement of risk tolerance and how the agency will assess, respond to, and monitor risks. Ten agencies stated that they faced challenges in establishing an agency-wide risk tolerance statement, while five noted that they faced challenges in implementing a strategy across the agency. For example:

- Education's Audit Liaison Officer from its Office of the CIO noted that it was a challenge to develop an enterprise-level statement of risk tolerance and that currently risk tolerance decisions were made at the system level by the authorizing official.
- EPA's CISO reported that it was challenge to establish an agency-wide statement of risk tolerance. This is because it was difficult to determine such factors as how much the mission's operation is worth, how much information resources are worth, and how much negative public perception of the agency costs in terms of money or resources.

NIST notes that framing risk through the creation of a cybersecurity risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within an agency.[28] If agencies are challenged in developing cybersecurity risk management strategies, they may be hindered in making consistent decisions for identifying, assessing, and responding to cybersecurity risks.

[28] NIST 800-39.

Incorporating Cyber Risks into Enterprise Risk Management

Fourteen of the 23 civilian CFO Act agencies reported that incorporating cyber risks into the enterprise risk management process was a challenge. Nine of these agencies noted challenges related to coordination between cybersecurity and ERM, such as establishing effective channels of communication or developing vocabularies for discussing risk that were understandable by all stakeholders. In addition, five agencies noted that their ERM process was still maturing. For example:

- GSA's Associate Chief Information Officer for Enterprise Planning & Governance stated that a process was implemented to assess cyber risks as part of the formalized ERM process; however, this official noted that additional work is still needed to align and incorporate other regular cybersecurity risk management reporting processes and communication channels into the broader ERM framework.
- Treasury's Enterprise Cybersecurity Risk Management Officer stated that incorporating cyber risks into ERM is a challenge because cybersecurity risk is not currently quantified in the same way as other risks. The official expressed the need for a standard vocabulary for discussing cyber alongside other risks, adding that this makes it very challenging to integrate cybersecurity risk management into ERM.

OMB has stated that an effective enterprise risk management program promotes a common understanding for recognizing and describing potential risks that can impact an agency's mission and the delivery of services to the public. Such risks include strategic, market, cyber, legal, reputational, political, and a broad range of operational risks.[29] If agencies do not successfully integrate cyber risks into their ERM processes, they may be hindered in making effective decisions about addressing cybersecurity risks in the context of other risks and their potential impact on agency missions.

[29] OMB M-17-25.

OMB and DHS Took Steps to Improve Cybersecurity Risk Management; Current Initiatives Address Some but Not All Identified Challenges

In accordance with a recent executive order, OMB and DHS took steps to assess agencies' cybersecurity management capabilities. They also identified core actions to be taken, in coordination with agencies, to address cybersecurity risks across the executive branch. Accordingly, OMB and DHS have several initiatives under way to address these risks, and several of these initiatives should help address some of the challenges in establishing cybersecurity risk management programs that the agencies in our review identified. However, these initiatives do not address other challenges identified by a majority of the agencies.

OMB and DHS Assessed Government-Wide Cybersecurity Risks and Identified Findings Related to Federal Cybersecurity

EO 13800 on *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* emphasizes the importance of reducing cybersecurity risks while also providing exceptional service to the public. The EO aligns with FISMA by holding agency heads accountable for managing cybersecurity risks. Toward this end, it directed agency heads to provide a risk management report to OMB and DHS that documented the agency's risk mitigation and acceptance choices as of May 2017 and describe the agency's action plan to implement the NIST cybersecurity framework.

The EO required OMB and DHS to assess each agency's risk management report and OMB, in coordination with DHS, to develop and deliver a risk determination report to the President on whether the risk mitigation and acceptance choices set forth in the agencies' reports were appropriate and sufficient to manage the cybersecurity risk to the executive branch as a whole. OMB's and DHS's report was also to include an action plan to, among other things,

- adequately protect the executive branch, should the risk determination identify insufficiencies in agencies' risk mitigation and acceptance choices;

- establish a regular process to reassess and, if appropriate, reissue the determination and address future recurring and unmet budgetary needs necessary to manage risk to the executive branch; and
- if appropriate, clarify, reconcile, and reissue policies, standards, and guidelines issued in furtherance of FISMA and the EO, and align them with the NIST cybersecurity framework.

In May 2017, OMB issued guidance to agencies for implementing the provisions in EO 13800 on managing cybersecurity risks.[30] This guidance required agencies to, among other things, report on their cybersecurity risk management capabilities using the metrics established for monitoring FISMA implementation. OMB and DHS used the results of the agencies' risk management reports and responses to the FISMA reporting metrics[31] to assess agencies' capabilities and make risk determinations of agencies' performance ("high risk," "at risk," or "managing risk"). OMB and DHS's process included an assessment of 96 agencies across the executive branch, including the 23 civilian CFO Act agencies in the scope of our review.

In May 2018, OMB published the *Federal Cybersecurity Risk Determination Report and Action Plan*, in which OMB and DHS determined that 74 percent of the federal agencies participating in the risk assessment process had cybersecurity programs that were either "at risk" or "high risk." The report identified four key findings and actions necessary to address cybersecurity risks across the federal enterprise, as summarized in table 6. The report also described OMB's plans to work with DHS and other federal entities to implement these actions and reduce cybersecurity risks across the government.

[30] OMB, *Memorandum for the Heads of Executive Departments and Agencies: Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Infrastructure*, M-17-25 (Washington, D.C.: May 19, 2017).

[31] The FISMA reporting metrics are developed by DHS and OMB in collaboration with agencies and include both agency CIO and Inspector General perspectives on the maturity of agencies' information security programs.

Table 6: Findings on Cybersecurity Risks across the Federal Government from the Office of Management and Budget's Risk Determination Report and Action Plan

Finding	Description
Limited situational awareness	Agencies often lack timely information regarding the tactics, techniques, and procedures that threat actors use to exploit government information systems.
Lack of standardized IT capabilities	Agencies do not have standardized cybersecurity processes and IT capabilities, which impacts their ability to efficiently gain visibility into and effectively combat threats.
Limited network visibility	Agencies lack visibility into what is occurring on their networks in order to effectively detect data exfiltration attempts and respond to cybersecurity incidents.
Lack of accountability for managing risks	Agency leadership above the chief information officer level may not be engaged in cybersecurity risk management and agencies do not possess robust risk management programs or consistent methods of notifying leadership of cybersecurity risks.

Source: OMB *Federal Cybersecurity Risk Determination Report and Action Plan*. | GAO-19-384

OMB and DHS also established a process for reassessing and, if necessary, reissuing the agency risk determinations.[32] Specifically, OMB and DHS use the metrics collected during the FISMA reporting process to update each agency's risk management assessment on an ongoing basis. At a minimum, CFO Act agencies must update their metrics quarterly. The quarterly risk management assessment process allows for the monitoring of agency-level risks, and OMB issues guidance yearly codifying this process.[33] In addition, OMB staff stated that they plan to incorporate the overall risk determination into the office's annual FISMA report to Congress, although they noted that this is subject to change.

Further, OMB and DHS took steps to align government-wide cybersecurity guidance with the NIST cybersecurity framework. For

[32] EO 13800 required OMB and DHS to deliver a risk determination report to the President on whether the risk mitigation and acceptance choices set forth in agency reports were appropriate and sufficient to manage the cybersecurity risk to the executive branch as a whole.

[33] OMB, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*, M-18-02 (Washington, D.C.: October 16, 2017) and OMB, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management* Requirements, M-19-02 (Washington, D.C.: October 25, 2018).

example, OMB and DHS, in coordination with the federal cybersecurity community, updated the reporting guidance on CIO and Inspector General FISMA metrics to align with the framework. The FISMA metrics leverage the framework as a standard for managing and reducing cybersecurity risks, and the metrics are aligned with the five main functions of the framework to provide agencies with a comprehensive structure for making more informed, risk-based decisions, managing cybersecurity risks across their enterprise, and providing a view of agencies' capabilities and potential gaps.

OMB and DHS Have Several Initiatives Under Way That Can Help Address Some, but Not All, Agency-Identified Challenges

OMB and DHS have several initiatives under way—some of them also outlined in OMB's federal cybersecurity report—that can assist agencies in meeting challenges related to hiring and retaining cybersecurity risk management personnel, establishing standardized IT capabilities, receiving quality data, and using NIST and OMB guidance.

- **Workforce education initiatives:** In November 2018, OMB announced the launch of the Federal Cyber Reskilling Academy pilot program, which is being sponsored by the CIO Council.[34] This program offers current federal employees who do not work in the IT field the opportunity for hands-on training in cybersecurity for 3 months to help them build foundational skills in cyber defense analysis. In addition, the National Initiative for Cybersecurity Careers and Studies is an online resource for cybersecurity training managed by DHS that connects government employees, students, educators, and industry with cybersecurity training providers throughout the nation.[35] The initiative's Federal Virtual Training Environment, for example, is an on-demand cybersecurity training system that contains more than 800 hours of training on a variety of topics, including risk management.

  These initiatives, if effectively implemented, could help address challenges agencies identified in hiring and retaining cybersecurity risk management personnel. Specifically, the Cyber Reskilling

[34] See https://www.cio.gov/reskilling.

[35] See https://niccs.us-cert.gov/about-niccs/niccs.

Academy has the potential to increase the pool of federal employees with skills that agencies need for cyber risk management. In addition, the Federal Virtual Training Environment can enhance federal employees' knowledge of and skills in cybersecurity risk management.

- **Continuous Diagnostics and Monitoring (CDM):** DHS's CDM initiative is to provide federal agencies with tools and services that have the intended capability to automate network monitoring, correlate and analyze security-related information, and enhance risk-based decision making at agency and government-wide levels. These tools include sensors that perform automated scans or searches for known cyber vulnerabilities, the results of which can feed into a dashboard that, at an agency level, is intended to alert network managers and enable the agency to allocate resources based on the risk. Summary data from each participating agency's dashboard is expected to be transmitted to the Federal Dashboard, where the data can be used to inform decisions about cybersecurity risks across the federal government. A DHS CDM program official stated that the department plans to continue to deploy capabilities in fiscal year 2019 for asset management, identity and access management, and monitoring network controls and activity.[36]

  The CDM initiative, if effectively implemented, has the potential to assist in addressing challenges agencies identified in establishing standardized IT capabilities for cybersecurity risk management and improving the quality of data to provide visibility into cyber risks. In particular, the tools and services offered through the program can provide agencies with standardized capabilities for collecting and analyzing cyber risk information. In addition, automated network monitoring and analysis can help agencies that currently must manually collect data from components based on self-reporting. Such data may be less timely and accurate than those collected through the tools available through CDM.

- **Security operations center (SOC) consolidation and maturation:** A SOC defends an organization against unauthorized activity within computer networks, including, at a minimum, detecting, monitoring, and analyzing suspicious activity. According to OMB, CISOs report that these centers do not communicate with each other and that they hoard, rather than share, threat information and intelligence. SOC

[36] According to DHS, CDM functionality is to include capabilities for asset management, identity and access management, monitoring network controls and activity, and data protection management.

consolidation focuses on centralizing information sharing across the agency, which is intended to improve the data agencies receive to provide visibility into cybersecurity risks. OMB and DHS are working with agencies to assess and enhance the maturity of their SOCs and streamline security operations across their enterprise. Specifically, agencies are required to develop and submit a Cybersecurity operations maturation plan to OMB and DHS by April 2019. Following submission of the plan, agencies are then required to complete SOC maturation, consolidation, or migration to a SOC-as-a-Service provider by September 2020.

Similar to CDM, SOC consolidation and maturation initiatives may help address challenges related to standardizing capabilities and collecting quality data, while enhancing enterprise-wide visibility. Consolidation can provide agencies with a standardized set of SOC services, while maturation can increase the quality of data on risks by establishing a baseline set of expected SOC capabilities for executive branch agencies.

- **Cyber threat framework:** OMB and DHS are developing and disseminating a framework, working with the Department of Defense, Office of the Director of National Intelligence, and the National Security Agency, to enable consistent characterization and categorization of cyber threat events. Specifically, the Cyber Threat Framework provides a hierarchical, structured, transparent, and repeatable methodology for characterizing adversarial activities in a standardized way across the federal government. The framework and the related methodology provide for a cybersecurity architecture review that allows an agency to assess its cyber capabilities against its actual threat environment. This includes a gap analysis to determine where agencies may need to enhance their capabilities to defend against key threats. To foster the adoption of the Cyber Threat Framework across the government, DHS—in coordination with OMB and the Department of Defense—intends to develop and implement a solution that will be available for agencies to use by the end of December 2019.

  The Cyber Threat Framework, if effectively implemented by civilian federal agencies, can also help address agency challenges related to the quality of data about cyber risks. By providing a standardized framework for understanding cyber threats, it is intended to assist agencies to better identify and prioritize risks, as well as the gaps in their capabilities for protecting against such threats.

- **Inter-agency cyber-focused working groups:** In coordination with DHS, OMB established CyberStat review sessions to assist agencies in protecting their systems, networks, and data. Specifically, agency cyber professionals, from the working level to the CIO, meet with DHS subject matter experts to participate in working sessions throughout a 4- to 6-week period to overcome barriers to success in specific cybersecurity programs. During a CyberStat review, DHS provides agencies with guidance on best practices and connects them with other subject matter experts who can provide advice on implementing the NIST framework and cybersecurity risk management practices. In addition, the federal CIO Council has recently issued the *CISO Handbook*, which was created to educate and inform new and existing CISOs about their role in federal cybersecurity. The council is the principal interagency forum for improving agency practices related to the use, sharing, and performance of federal information resources and part of its governing principles are to adopt and share IT management best practices and to manage risk and ensure privacy and security. Within the CIO Council, the CISO Council is specifically tasked with developing IT security policy and sharing best practices to improve the cybersecurity posture of the United States. Among other things, the *CISO Handbook* includes information on NIST's cybersecurity framework and how it can be leveraged in conjunction with other NIST risk management publications.

CyberStat reviews and the federal CIO Council can provide channels to help agencies in better understanding and implementing guidance from NIST and OMB on cybersecurity risk management. By connecting agencies with best practices and subject matter experts, CyberStat sessions are intended to help agencies, for example, apply the NIST framework and cyber risk management practices. In addition, the CIO Council, through sharing of best practices and issuing publications, can provide guidance on how to more effectively implement federal cybersecurity risk management guidance.

Although the initiatives under way could address challenges related to hiring and retaining cybersecurity risk management personnel, developing standardized capabilities, acquiring quality data about cyber risks, and using NIST and OMB guidance, the existing initiatives do not address challenges related to managing competing priorities, establishing consistent policies and procedures, incorporating cyber risks into enterprise risk management, and developing an agency-wide strategy for managing cybersecurity risks.

- **Managing competing priorities between cybersecurity and operations:** OMB staff stated that its newly developed risk-based budgeting model could help agencies prioritize their cybersecurity investments. This model is intended to tie agencies' cybersecurity spending to the FISMA metrics process in order to identify capability and process gaps that pose risks to an agency. OMB plans to disseminate the risk-based budgeting process to enable agency CIOs, CISOs, and Chief Financial Officers to communicate cyber risks effectively across their agencies and to budget strategically for cyber capabilities that address the agency's most critical cybersecurity needs. OMB anticipates being able to provide agencies with additional details surrounding this model in the cybersecurity section of its upcoming fiscal year 2020 guidance to the President's budget.

However, while this risk-based approach to cybersecurity budgeting should help agencies prioritize their cybersecurity investments, it does not address issues related to prioritizing between cybersecurity and mission or operational needs. The agencies in our review highlighted that mission or operational priorities can conflict with cybersecurity requirements when, for example, components within an agency have differing views about the relative importance of mission and cybersecurity activities. These issues do not relate to prioritizing investments in cybersecurity but to managing conflicts, or potential conflicts, between cybersecurity and mission needs.

- **Implementing consistent cybersecurity risk management policies and procedures:** OMB staff stated that several of OMB's and DHS's initiatives emphasize driving performance through centralized visibility, authority, and reporting. For example, OMB staff stated CDM is intended to establish agencies' visibility across the enterprise, as well as government-wide visibility. OMB staff stated the implementation of provisions commonly referred to as the Federal Information Technology Acquisition Reform Act is intended to enhance the role and authority of agency CIOs, particularly with respect to relationships with agency components and accountability for IT costs, performance, and security.[37] Additionally, OMB staff stated the risk management assessment process established in response to EO 13800 emphasizes centralized visibility, authority, and reporting.

While these efforts could provide increased visibility and CIO authority, they do not address factors identified by agencies that affected their ability to implement consistent cybersecurity risk management policies and procedures. These include differing views among staff regarding the importance of risks, and frequent changes in leadership, all of which, according to agencies, make consistency difficult to achieve.

- **Incorporating cyber risks into ERM:** While existing OMB guidance requires agencies to establish ERM programs and NIST guidance requires agencies to establish cybersecurity risk management programs, this guidance does not address how these efforts should be integrated or coordinated. For example, OMB A-123 outlines agencies' responsibilities for establishing an ERM capability but does not specifically address how enterprise risk management should incorporate cyber risks. In addition, NIST guidance on cybersecurity risk management recognizes that cybersecurity can be an important component of an organization's overall risk management and states that its information security risk management guidance should be used as part of a more comprehensive ERM program. However, it does not explicitly discuss how to integrate or coordinate cybersecurity risk management and enterprise risk management.

[37] Recognizing the severity of issues related to the government-wide management of IT, in December 2014, Congress enacted IT acquisition reform legislation (commonly referred to as the *Federal Information Technology Acquisition Reform Act*, or FITARA) as part of the *Carl Levin and Howard P. 'Buck' McKeon National Defense Authorization Act for Fiscal Year 2015*, Pub. L. No. 113-291, Div. A, Title VIII, Subtitle D, 128 Stat. 3292, 3438-50 (Dec. 19, 2014). FITARA was intended to improve covered agencies' acquisitions of IT and enable Congress to monitor their progress, as well as hold those agencies accountable for reducing duplication and achieving cost savings. In addition, with the enactment of FITARA, the federal government is to strengthen the authority of chief information officers (CIO) to provide needed direction and oversight of covered agencies' IT budgets. In June 2015, OMB released FITARA guidance (referred to as the "common baseline"). OMB, *Management and Oversight of Federal Information Technology*, M-15-14 (Jun. 10, 2015). The common baseline describes how covered agencies are to implement the requirements of the law through the use of management controls, including controls related to the development of IT budgets. The guidance identifies a number of actions that agencies are to take to establish a basic set of roles and responsibilities (the common baseline) for CIOs and other senior agency officials.

- **Establishing a cybersecurity risk management strategy:** OMB noted that the cyber threat framework will provide a more tangible way for agencies to identify and prioritize cyber risks. However, while this framework will allow agencies to better identify and categorize threats and the capabilities needed to counter them, it does not address key aspects of risk framing such as establishing an agency-wide statement of risk tolerance and acceptable risk mitigation strategies. Several agencies noted that they struggled to define risk tolerance and establish criteria for different risk responses that could provide a consistent, agency-wide approach to risk management.

Without additional guidance or other processes to identify successful approaches for addressing these challenges, agencies will continue to be hindered in establishing programs for effectively managing their cybersecurity risks.

Conclusions

Given the increasing number and sophistication of cyber threats facing federal agencies, it is critical that agencies are well positioned to make consistent, informed risk-based decisions in protecting their systems and information against these threats. While all the agencies in our review have taken steps to establish cybersecurity risk management programs, they have not fully addressed key practices that are foundational to effectively managing cybersecurity risks. In particular, without developing an agency-wide cybersecurity risk management strategy, agencies may lack a consistent approach to managing cybersecurity risks. In addition, while agencies have documented policies and procedures that include many key practices, gaps remain that may hinder their ability to ensure a consistent implementation of risk-based practices. Further, without a process for an agency-wide cybersecurity risk assessment, agencies may be missing opportunities to identify risks that affect their entire organization, and to implement solutions to address them. Finally, establishing processes for coordinating cybersecurity risk information with the entity responsible for enterprise risk management would help ensure that cyber risks are being considered by senior leadership in the context of other risks facing the agency.

This inconsistent establishment of cybersecurity risk management practices can be partially attributed to challenges agencies identified in establishing and implementing their cybersecurity risk management programs. Specifically, agencies noted a variety of challenges such as hiring qualified staff, competing priorities between cybersecurity and mission needs, implementing consistent policies and procedures, incorporating cyber risks into enterprise risk management processes, and developing a cybersecurity risk management strategy. Addressing these challenges will be an important step toward establishing more effective cybersecurity risk management programs across the 23 agencies.

OMB and DHS have taken steps to carry out their responsibilities to identify and address weaknesses across the executive branch, including actions that would address many of the challenges identified by agencies. However, without fully addressing challenges related to prioritization between cybersecurity needs and mission priorities, implementing consistent risk management policies and procedures, incorporating cyber risks into enterprise risk management, and establishing a cybersecurity risk management strategy, OMB and DHS are likely to be missing opportunities to assist agencies in these key areas. Clarified or updated guidance, along with sharing successful practices or lessons learned, could help agencies more fully establish their cybersecurity risk management capacity.

Recommendations for Executive Action

We are making the following recommendation to OMB:

- The Director of OMB should, in coordination with the Secretary of Homeland Security, establish guidance or other means to facilitate the sharing of successful approaches for agencies to address challenges in the areas of (1) managing competing priorities between cybersecurity and operations, such as when operational needs appear to conflict with cybersecurity requirements; (2) implementing consistent cybersecurity risk management policies and procedures across an agency; (3) incorporating cyber risks into enterprise risk management, and (4) establishing agencies’ cybersecurity risk management strategies. (Recommendation 1)

We are also making a total of 57 recommendations to the 23 civilian CFO Act agencies in our review to fully address key practices in their cybersecurity risk management policies and procedures. Appendix VII contains these recommendations.

Agency Comments and Our Evaluation

We requested comments on a draft of this report from OMB and the 23 civilian CFO Act agencies included in our review. All the agencies provided responses, as further discussed.

In an email from the office's GAO audit liaison on July 8, 2019, OMB did not state whether it agreed or disagreed with our recommendations. However, the office provided technical comments, which we incorporated as appropriate.

Of the 23 civilian CFO Act agencies, 17 agencies (Education, Energy, DHS, HUD, Interior, Labor, State, Transportation, VA, USAID, GSA, NASA, NSF, NRC, OPM, SBA, and SSA) concurred with our recommendations; one agency (HHS) partially concurred with our recommendations; three agencies (Commerce, Justice, and Treasury) provided comments but did not state whether they agreed or disagreed with our recommendations; and two agencies (Agriculture and EPA) stated that they had no comments on the report. Multiple agencies also provided technical comments, which we incorporated as appropriate.

The following 17 agencies concurred with our recommendations and, in most cases, described steps planned or under way to address them:

- The Department of Education provided written comments in which it concurred with our recommendation and stated that the department will continue its efforts to fully develop a cybersecurity risk management strategy that includes the definition of risk tolerance and acceptable risk response strategies. Education's comments are reprinted in appendix VIII.
- The Department of Energy provided written comments in which it concurred with our two recommendations and described steps and time frames for addressing them. In one case, regarding our recommendation to update the department's policies to address missing elements, Energy stated that, as of May 2019, it had already completed an update of its policies to implement this recommendation. We intend to follow up with the department and obtain and assess evidence to determine its implementation of this recommendation. Energy's comments are reprinted in appendix IX.
- In written comments, the Department of Homeland Security stated that it was pleased that our report noted steps that DHS and OMB

have taken to improve agencies' capabilities for managing cyber risks. DHS also concurred with our two recommendations and described steps it intends to take to address them, along with estimated completion dates. DHS's comments are reprinted in appendix XI. The department also provided technical comments, which we have incorporated as appropriate.

- The Department of Housing and Urban Development provided written comments in which it thanked GAO for the opportunity to review the report and stated that it concurred with the recommendations. HUD's comments are reprinted in appendix XII.
- The Department of the Interior provided written comments in which it concurred with our three recommendations. Interior also described planned steps to address the recommendations, such as developing a cybersecurity risk management strategy that includes the key elements and updating its policies. The department's comments are reprinted in appendix XIII.
- In written comments, the Department of Labor concurred with our recommendation. Labor stated that it intends to take necessary steps to update the department's policies. The department's comments are reprinted in appendix XIV.
- The Department of State provided written comments in which it concurred with our two recommendations. State also described steps planned or under way to address the recommendations. For example, State described ongoing policy updates to address control monitoring, system-level risk assessments, and the use of risk assessments to inform control tailoring. It also described ongoing steps to align its cybersecurity risk management activities with its ERM governance structure. State's comments are reprinted in appendix XV.
- The Department of Transportation's Director of Audit Relations & Program Improvement provided comments via email on June 25, 2019, which stated that the department concurs with the findings and recommendations in the draft report.
- The Department of Veterans Affairs provided written comments in which it concurred with our four recommendations. VA also described actions planned or under way to address the recommendations. Regarding our recommendation to establish and document a process for coordination between its cybersecurity and enterprise risk management functions, the department stated that it had already established such a process and requested closure of the recommendation. We intend to follow up with the department and

obtain and assess evidence to determine if its actions fully address our recommendation. VA’s comments are reprinted in appendix XVI.

- The U.S. Agency for International Development provided written comments in which it agreed with our two recommendations. USAID also described steps it has planned or under way to address the recommendations, such as amending its guidance to address an organization-wide cybersecurity risk assessment. The agency’s comments are reprinted in appendix XVII.
- In written comments, the General Services Administration stated that it appreciated the opportunity to review the report and concurred with its findings. The agency added that it is implementing an action plan to address the four recommendations. GSA’s comments are reprinted in appendix XVIII.
- The National Aeronautics and Space Administration provided written comments in which it concurred with our two recommendations. NASA also described planned steps to address the recommendations, such as updating its policies and establishing a process for an organization-wide cybersecurity risk assessment, along with estimated completion dates. The agency’s comments are reprinted in appendix XIX.
- The National Science Foundation’s GAO liaison provided comments via email on July 3, 2019, which stated that the agency concurred with our recommendation and intends to update its cybersecurity risk management strategy to address the missing elements.
- The Nuclear Regulatory Commission provided written comments in which it stated that the agency was in general agreement with the findings and recommendations in our draft report. NRC’s comments are reprinted in appendix XX.
- The Office of Personnel Management provided written comments in which it stated that it concurred with our two recommendations. OPM also described planned steps to address the recommendations, such as updating its policies and establishing a process for an organization-wide cybersecurity risk assessment. The agency’s comments are reprinted in appendix XXI.
- In written comments, the Small Business Administration concurred with our three recommendations. SBA described steps planned or under way to address the recommendations, such as updating its cybersecurity risk management strategy and policies and establishing a process for an organization-wide cybersecurity risk assessment, along with estimated completion dates. The agency’s comments are reprinted in appendix XXII.

- In written comments, the Social Security Administration agreed with our recommendation and described planned efforts to further integrate its cybersecurity and enterprise risk management functions. SSA's comments are reprinted in appendix XXIII.

One agency—the Department of Health and Human Services—concurred with three of our recommendations and partially concurred with one recommendation. Specifically, HHS concurred with our recommendations to develop a risk management strategy that includes key elements, establish a process for conducting an agency-wide cybersecurity risk assessment, and establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. Further, HHS described steps planned or under way to address these recommendations.

Regarding our recommendation to update department policies to require an organization-wide cybersecurity risk assessment and the use of risk assessments to inform control tailoring, HHS stated that it concurred with the first part of the recommendation, but did not concur with the second part of the recommendation. Specifically, the department described steps it has planned or under way to update its policies to require an organization-wide risk assessment, in accordance with the first part of the recommendation. With respect to the second part of the recommendation, the department pointed to portions of its information security and privacy policy that address the selection of security and privacy controls.

However, while these policy statements require adherence to NIST and OMB standards for selecting security controls and require a rationale for tailoring decisions, they do not specifically require the use of risk assessments to inform the tailoring of security controls. As NIST states, organizations apply the tailoring process to align the controls more closely with the specific conditions within the organization and should use risk assessments to inform and guide the tailoring process for organizational information systems and environments of operation. Making this requirement explicit in policy would help HHS ensure that it is applying the appropriate set of controls to its systems; thus, we maintain that our recommendation is still warranted.

HHS's comments are reprinted in appendix X. The department also provided technical comments, which we incorporated as appropriate.

We received technical comments via email from the GAO audit liaisons at three agencies—the Department of Commerce (on June 21, 2019), the

Department of Justice (on July 8, 2019), and the Department of the Treasury (on July 3, 2019). The agencies did not state whether they agreed or disagreed with our recommendations. We incorporated their technical comments as appropriate.

We received emails from Agriculture's Director of Strategic Planning, Egovernment and Audits on June 19, 2019, and from a Division Director in the Environmental Protection Agency's Office of Information Security and Privacy on July 8, 2019, which stated that their agencies had no comments on the draft report.

We are sending copies of this report to the appropriate congressional committees, the heads of the agencies in our review, and other interested parties. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-9342 or marinosn@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 XXIV.

Nick Marin

Nick Marinos
Director, Information Technology & Cybersecurity

List of Requesters

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
The Honorable Elijah E. Cummings
Chairman
The Honorable Jim Jordan
Ranking Member
Committee on Oversight and Reform
House of Representatives
The Honorable Thomas R. Carper
United States Senate

The Honorable Susan Collins
United States Senate

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to examine

(1) the extent to which agencies established key elements of a cybersecurity risk management program;

(2) what challenges, if any, agencies identified in developing and implementing cybersecurity risk management programs; and

(3) what steps the Office of Management and Budget (OMB) and Department of Homeland Security (DHS) have taken to meet their risk management responsibilities under Executive Order (EO) 13800[1] and to address any challenges agencies face in implementing cybersecurity risk management practices.

In conducting this engagement, we focused on 23 of the 24 agencies covered by the *Chief Financial Officers Act of 1990*.[2] To address our first objective, we collected agency policies, procedures, and other documentation and compared them to selected key practices from OMB and National Institute of Standards and Technology (NIST) guidance for cybersecurity risk management.

To identify the key practices, we reviewed OMB guidance pertaining to cybersecurity risk management, including OMB Circular A-130: *Managing*

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

[2] These agencies are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the U.S. Agency for International Development; Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulatory Commission; Office of Personnel Management; Small Business Administration; and the Social Security Administration. We excluded the Department of Defense from our review because the information we requested pertaining to cybersecurity risk management was classified, therefore not available in a public report. 31 U.S.C. § 901(b).

Information as a Strategic Resource,[3] as well as Circular A-123: *Management's Responsibility for Enterprise Risk Management and Internal Control*,[4] which outlines agency responsibilities for enterprise risk management. We also reviewed NIST guidance, including the *Framework for Improving Critical Infrastructure Cybersecurity*;[5] Special Publication 800-30: *Guide for Conducting Risk Assessments*;[6] Special Publication 800-37: *Guide for Applying the Risk Management Framework to Federal Information Systems*,[7] and Special Publication 800-39: *Managing Information Security Risk: Organization, Mission, and Information System View*.[8] In selecting the key practices for our assessment, we focused on those practices identified by OMB and NIST as foundational for providing an organization-wide approach to cybersecurity risk management.

We collected and analyzed documentation and other information from each agency related to cybersecurity risk management and compared it to the identified key practices. We supplemented our analyses with interviews with relevant agency officials to discuss the development of their policies. We discussed the results of our initial analysis of agency documentation with agency officials to validate our findings, collect additional evidence, and identify causes for any gaps. We then determined whether the evidence provided by the agency addressed

[3] OMB Circular A-130: *Managing Information as a Strategic Resource* (Washington, D.C.: July 2016).

[4] OMB Circular A-123: *Management's Responsibility for Enterprise Risk Management and Internal Control* (Washington, D.C.: July 2016).

[5] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, Md.: April 2018).

[6] NIST, *Guide for Conducting Risk Assessments*, SP 800-30, Revision 1 (Gaithersburg, Md.: September 2012).

[7] NIST, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Lifecycle Approach,* SP 800-37, Revision 1 (Gaithersburg, Md.: February 2010, updated June 2014). In 2018, NIST released a draft revision 2 of 800-37 for public comment. Among other things, this revision emphasizes the importance of key organization-level practices to create a foundation for more effective, efficient, and cost-effective risk management. NIST published the final version of revision 2 in December 2018, which supersedes revision 1. See *Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy*, NIST SP 800-37 Revision 2 (December 2018). Revision 1 of SP 800-37 is to be officially withdrawn on December 20, 2019.

[8] NIST, *Managing Information Security Risk: Organization, Mission, and Information System View,* SP 800-39 (Gaithersburg, Md.: March 2011).

each identified criteria element. Specifically, for each criteria element, we determined if the evidence fully addressed the element ("met"), addressed some, but not all, aspects of the element ("partially met"), or did not address any aspects of the element ("not met").

To address the second objective, we administered structured interview questions to the agencies to determine what challenges, if any, they face in developing and implementing policies and procedures for managing cybersecurity risk. We developed a list of potential challenges based on our assessment of agencies' policies and procedures, a review of OMB's risk report on agencies' cybersecurity risk management capabilities,[9] and reviews of prior GAO reports in areas related to cybersecurity risk management. We worked with GAO methodologists to develop a set of structured interview questions that were sent to the agencies and asked them to indicate if they faced each of these, as well as any additional, challenges, and to provide specific examples. We received responses from all 23 agencies in our review and analyzed them to identify those challenges that were indicated by a majority of the agencies. We excluded from our counts agencies that stated they did not have challenges in a particular area. We also identified common themes within the challenge areas.

To address the third objective, we reviewed EO 13800 and implementation guidance issued by OMB,[10] as well as relevant reports and other documents, including OMB's *Federal Cybersecurity Risk Determination Report and Action Plan*, OMB memos, and supporting documentation for DHS initiatives. We also interviewed OMB and DHS officials with government-wide cybersecurity responsibilities to gain an understanding of initiatives under way to address their responsibilities under the order, and that could help address challenges identified by the agencies. We then compared these initiatives to the responses we received from agencies to determine if there were any gaps between the challenges and the ongoing initiatives. Specifically, for each challenge

[9] OMB, *Federal Cybersecurity Risk Determination Report and Action Plan* (Washington, D.C.: May 2018).

[10] Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (Washington, D.C.: May 2017); OMB M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (Washington, D.C.: May 2017); and OMB M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements* (Washington, D.C.: October 2018).

identified by a majority of the agencies in our review, we determined if any of the initiatives under way would address them based on a review of documentation associated with the initiatives as well as discussions with OMB and DHS officials.

We conducted this performance audit from February 2018 to July 2019 in accordance with generally accepted government auditing standards. 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.

Appendix II: Details on the Extent to Which Agencies Established a Cybersecurity Risk Executive Function

Twenty-two of the 23 civilian Chief Financial Officers Act agencies in our review established and documented the role of the cybersecurity risk executive. Agencies varied in assigning this responsibility to the chief information officer (CIO), chief information security officer (CISO), or another official or entity. Table 7 provides details on our assessment.

Table 7: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Established a Cybersecurity Risk Executive

Agency	Assessment	Discussion
Department of Agriculture	Met	The department's Chief Information Security Officer (CISO) serves as the risk executive and is to have the authority to enforce compliance with all federal and departmental information security requirements in order to effectively manage information security risks to the department's mission and assets.
Department of Commerce	Met	The department's Office of Cyber Security and IT Risk Management is the risk executive function for department-wide cybersecurity; oversight for this office is provided by the CISO. Through the management of cybersecurity solutions and services, cybersecurity reporting and analytics, and the delivery of IT risk management programs, the Office of Cyber Security and IT Risk Management is responsible for effective oversight of cybersecurity and information technology risk for the department.
Department of Education	Met	According to the department's Information Assurance and Cybersecurity Policy, the Chief Information Officer (CIO) is the senior official responsible for management of assets, data, and information resources within the department and develops, oversees, and manages its cybersecurity mission. The CIO is to ensure that an information risk management strategy is established and implemented and provides oversight of all department-wide risk related activities.
Department of Energy	Met	The department's Cyber Council serves as the risk executive. The focus of the Cyber Council is to ensure enterprise-wide compliance with standards for cybersecurity and risk management. The council is to ensure that the department's cybersecurity program and risk management approach are aligned with mission requirements and department management principles.
Department of Health and Human Services	Met	At the Department of Health and Human Services, the CIO serves as the risk executive for the department and is responsible for executing the risk management framework tasks outlined in NIST SP 800-37.
Department of Homeland Security	Met	The departmental risk executive function has been delegated by the Department of Homeland Security (DHS) CIO to the DHS CISO. Responsibilities for the risk executive include providing visibility into the decisions of authorizing officials and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems,

Agency	Assessment	Discussion
Department of Housing and Urban Development	Met	The Department of Housing and Urban Development (HUD) CIO serves as the department's cybersecurity risk executive. According to the department's IT security policy, the risk executive is to ensure that management of information system-related security risks is consistent across HUD, reflects organizational risk tolerance, and is performed as part of a HUD-wide process that considers other organizational risks affecting mission/business success.
Department of the Interior	Met	The Department of the Interior CIO serves as the IT Risk Executive Officer and Senior Agency Official for Risk Management and reports directly to the Secretary.
Department of Justice	Met	The department designated the Assistant Director, Policy, Audit & Administration within the Office of the CIO as the risk executive who reports to the department CIO and CISO on all cybersecurity risks.
Department of Labor	Met	The department's senior accountable official for ensuring cybersecurity risk management, assigned as a result of Executive Order 13800, also serves as the agency's cybersecurity risk executive. The current senior accountable official for cybersecurity is the department's CIO.
Department of State	Met	The department designated its CISO as its cybersecurity risk executive. Responsibilities include coordinating with the designated risk officer for cyber to implement the mandated risk management program and establish agency-wide processes and practices that assess, quantify, and mitigate risks to department information and systems.
Department of Transportation	Met	The department's cybersecurity policy states that the responsibilities of the CIO include, among other things, performing the role of the department's risk executive unless otherwise specified by the Secretary of Transportation. The policy defines the role of the risk executive as an official or group that has the ability to link risk management processes at the information system level to risk management processes at the organization level. In addition, the department identified the deputy CIO as the senior accountable official for risk management.
Department of the Treasury	Met	The Department of the Treasury assigns the function of risk executive to its department CIO Council. Responsibilities include ensuring the cybersecurity program is consistent with the provisions of National Institute of Standards and Technology (NIST) Special Publication 800-39; providing guidance to and oversight of the agency's risk management program and developing the cybersecurity risk management strategy; communicating organization-wide threat, vulnerability, and risk-related information; and providing a strategic view for managing cyber risk throughout the organization.
Department of Veterans Affairs	Met	The department's CISO is to perform the risk executive function and is responsible for cybersecurity risk and implementation for the department. According to department policy, the CISO is responsible for, among other things, carrying out the responsibilities of the CIO under the *Federal Information Security Modernization Act (FISMA) of 2014*, to include establishing and issuing policies, risk-based control requirements, and other standards, as well as ensuring that facility CIOs and information security officers comply with all cybersecurity directives and mandates.
U.S. Agency for International Development	Met	The agency designated the CISO with responsibility for carrying out the risk executive functions for the agency. Among other things, the CISO is responsible for developing, implementing, and managing an agency-wide security authorization process and a threat awareness program.

Agency	Assessment	Discussion
Environmental Protection Agency	Met	The Environmental Protection Agency (EPA) Chief Information Officer serves as the agency's risk executive in coordination with the agency's Risk Executive Group. In conjunction with this group, the risk executive is responsible for (1) identifying the EPA-wide risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible, (2) providing oversight for all information security risk management-related activities across EPA to help ensure consistent and effective risk acceptance decisions, (3) facilitating the sharing of risk-related information among authorizing officials and other senior leaders across EPA, and (4) coordinating with Risk Executive Group members in leveraging continuous monitoring results to determine system-, mission-, and agency-level risks.
General Services Administration	Not met	The General Services Administration (GSA) did not define the role of its cybersecurity risk executive in its policy. Although GSA officials stated that the agency's risk executive responsibilities were shared among the CIO, CISO, authorizing officials, and other GSA officials for risk management, the agency has not clearly defined or formally documented these roles and responsibilities in agency policy.
National Aeronautics and Space Administration	Met	The Senior Agency Information Security Officer is to serve as the agency's Information System Risk Executive related to NIST requirements and is responsible for ensuring that security risk-related considerations and risk management of individual information systems are consistent across the agency, viewed from an agency-wide and strategic goal perspective, and reflect the agency's information system risk tolerance affecting mission/business success.
National Science Foundation	Met	The agency's CIO is the agency's cybersecurity senior accountable official for risk management.
Nuclear Regulatory Commission	Met	The agency's risk executive function is assigned to the CISO. The CISO is responsible for ensuring that risk acceptance decisions are consistent across the agency, identifying organizational risk posture based on aggregating risk from individual IT systems, and ensuring that cybersecurity is integrated into segmented enterprise architectures. The IT risk executive function integrates with the security authorization to provide consistency across the agency, reflect the agency's risk tolerance, and perform as part of an agency-wide process that considers other agency risks affecting mission or business success.
Office of Personnel Management	Met	According to the agency's Cybersecurity Risk Management Strategy, its Risk Management Council operates as the risk executive function and supports consistent and effective risk-based decisions with consideration for all types of risk. The agency's CISO is responsible for risk assessment, risk response, risk monitoring activities, and enterprise cybersecurity program risks.
Small Business Administration	Met	The agency's CIO serves as the agency's senior accountable official for risk management, with agency-wide responsibilities for cybersecurity risk management.
Social Security Administration	Met	The agency's Cybersecurity Policy states that the CISO is the agency's cybersecurity risk executive with responsibilities for the agency's IT security program and the Office of Information Security. Under the direction of the CISO, this office is responsible for IT risk management as a fundamental tenet of IT security.

Source: GAO analysis of agency data. | GAO-19-384

Appendix III: Details on the Extent to Which Agencies Developed a Cybersecurity Risk Management Strategy

Of the 23 civilian Chief Financial Officers Act agencies, seven fully established a cybersecurity risk management strategy that included key elements recommended by National Institute of Standards and Technology (NIST) guidance. Specifically, these seven agencies developed strategies to guide how cybersecurity risk is to be framed, assessed, responded to, and monitored. In addition, five of the 23 agencies partially developed a cybersecurity risk management strategy, but their strategies did not address certain required elements. The remaining 11 agencies did not develop an agency-wide cybersecurity risk management strategy. Table 8 provides details on our assessment.

Table 8: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Established a Cybersecurity Risk Management Strategy

Agency	Assessment	Discussion
Department of Agriculture	Not met	Department officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. However, the officials stated that they were in the process of developing a strategic plan that would address the elements of a cybersecurity risk management strategy.
Department of Commerce	Met	Department officials developed an Enterprise Risk Management Guidebook, which serves as the risk management strategy for the entire department. The strategy's approach provides a standardized means of addressing risk that applies to the entire organization including cyber issues, and the strategy includes an expression of organizational risk tolerance, and how the agency intends to assess, respond to, and monitor risk.
Department of Education	Partially met	The Department of Education developed a guide for its risk scorecard that described how the department assesses and monitors risk. However, the guide did not include a statement on risk tolerance and acceptable risk response strategies. Chief information officer (CIO) officials did not state whether they intended to update their strategy to address the missing elements.
Department of Energy	Not met	Department of Energy officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. The officials stated that they were considering the need to develop such a strategy.

Agency	Assessment	Discussion
Department of Health and Human Services	Not met	Department officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. They attributed this, in part, to the federated nature of the department and described steps they were taking, such as working on the process for establishing risk thresholds/triggers (escalation, management/leadership involvement/trade-offs) as part of deploying a centralized, comprehensive risk management, reporting, and tracking tool. The process includes establishing criteria and weights for risk scoring within the tool and defining risk tolerance as they gather more information.
Department of Homeland Security	Not met	Department officials provided strategy documents and policies that they stated constituted a strategy or parts of a strategy. However, these documents did not constitute an integrated strategy that addressed key elements such as risk tolerance and risk mitigation strategies.
Department of Housing and Urban Development	Not met	The department provided strategy documents and policies that they stated constituted a strategy or parts of a strategy. However, these documents did not constitute an integrated strategy that addressed key elements such as risk tolerance and risk mitigation strategies.
Department of the Interior	Not met	Department of Interior officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. Interior officials attributed this, in part, to recent changes in agency leadership and noted that they are in the process of updating organizational policies and procedures to include the development of a strategy.
Department of Justice	Not met	Department of Justice officials provided strategy documents and policies that they stated constituted a strategy or parts of a strategy. However, these documents did not constitute an integrated strategy that addressed key elements such as risk tolerance and risk mitigation strategies.
Department of Labor	Met	The Department of Labor created an IT-focused enterprise risk management strategy. The strategy discusses risk tolerance in terms of thresholds based on essential mission functions and the processing of personally identifiable information, among other factors. It also included tasks for assessing enterprise-level risks, a breakdown of risk response strategies, and requirements for a risk monitoring strategy and the monitoring of departmental information systems and environments on an ongoing basis.
Department of State	Met	The Department of State provided its Cybersecurity Risk Management Strategy. The strategy addresses risk tolerance, assessing risk, risk response, and monitoring risk over time.
Department of Transportation	Partially met	The Department of Transportation’s Security Authorization and Continuous Monitoring Guide and its Cybersecurity Compendium and Security Weakness Management Guide laid out aspects of the department’s risk management strategy, including how the agency intends to monitor risk; however, these documents do not include a definition of acceptable risk assessment methodologies, risk mitigation strategies, and an explicit statement of the department’s risk tolerance. Officials from the department’s office of the CIO stated that these elements were addressed in these and other agency documents, but they were not.
Department of the Treasury	Not met	Department of the Treasury officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements and stated that they were planning to create a risk management strategy before the end of fiscal year 2020.
Department of Veterans Affairs	Not met	Department of Veterans Affairs officials provided strategy documents and policies that they stated constituted a strategy or parts of a strategy. However, these documents did not constitute an integrated strategy that addressed key elements such as risk tolerance and risk mitigation strategies.
U.S. Agency for International Development	Met	Agency officials provided their cybersecurity Risk Management Plan, which addressed how the U.S. Agency for International Development is to address risk tolerance, risk assessment, risk response, and risk monitoring.

Agency	Assessment	Discussion
Environmental Protection Agency	Partially met	The Environmental Protection Agency's Information Security Risk Management Strategic Plan addressed all required elements with the exception of how the agency intends to assess risk. The agency's chief information security officer (CISO) acknowledged this element is not in the plan but is addressed within their risk assessment procedures. Further, the same official stated that the agency plans to include a reference to the risk assessment procedures in an update to their strategy.
General Services Administration	Met	The General Services Administration's IT Security Procedural Guide: Risk Management Strategy defined its approach to managing information security risks, including detailing its process for conducting risk assessments; defining its risk tolerance strategy based on factors such as system impact levels, types of data processed, and accessibility of systems; acceptable risk response strategies based on the criticality of identified vulnerabilities; and its approach to monitoring risk factors over time.
National Aeronautics and Space Administration	Not met	Agency officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. We previously recommended that the agency develop such a strategy[a] and the officials stated that they were developing one.
National Science Foundation	Partially met	The agency's IT Security Risk Management Strategy included how the agency intends to respond to risk; however, the strategy did not include a statement of risk tolerance and how the agency intends to assess and monitor risk. Agency IT and risk management officials did not state whether they intended to update their strategy to address the missing elements.
Nuclear Regulatory Commission	Not met	Agency officials acknowledged that they had not developed a cybersecurity risk management strategy that includes the key elements. The officials stated that they are drafting a cybersecurity framework that is intended to address its strategy, including an expression of risk tolerance and how the agency intends to access, respond to, and monitor risks over time.
Office of Personnel Management	Met	The Office of Personnel Management developed a cybersecurity risk management strategy that described how the agency will frame risk, including risk tolerance at different organizational levels; how it will assess risks, including how threats and vulnerabilities will be identified and risk determined; how risk response strategies will be selected based on risk tolerance; and how risk will be monitored over time.
Small Business Administration	Partially met	The Small Business Administration's Implementation Procedures for the National Institute of Standards and Technology's (NIST) Risk Management Framework addressed how the agency intends to assess risk; however it did not include a statement on risk tolerance, acceptable risk response strategies, or a discussion of how the agency intends to monitor risk. Agency officials stated that they believe their existing procedures address these elements in practice; however, they are not explicitly articulated in a strategy.
Social Security Administration	Met	The Social Security Administration developed a Cyber Risk Management Strategy, which provides the agency's risk management framework process and guidance for authorization decisions for information systems. The strategy includes a discussion of risk tolerance, risk response strategies, and how the agency will assess and monitor risk.

Source: GAO analysis of agency data. | GAO-19-384

[a] GAO, *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, GAO-18-337 (Washington, D.C.: May 2018).

Appendix IV: Details on the Extent to Which Agencies Developed Risk-Based Policies and Procedures

The following elements, identified in NIST guidance,[1] should be addressed in policies and procedures to facilitate risk-based decision making in securing information systems and data.

Table 9: Risk-Based Elements for Policies and Procedures

Identify and assign individuals to specific roles for executing the risk management framework.
Develop and update an organization-wide cybersecurity risk assessment.
Identify, document, and publish common controls that are available for inheritance by organizational systems. Common controls are controls that can be inherited by one or more information systems. Organizations identify and select the set of common controls and allocate those controls to the organizational entities designated as common control providers.
Develop and implement an organization-wide strategy for monitoring control effectiveness. The continuous monitoring strategy identifies the minimum monitoring frequency for implemented controls across the organization; defines the ongoing control assessment approach; and describes how ongoing assessments are to be conducted.
Conduct and regularly update system-level risk assessments. Assessment of security risk includes identification of threat sources and threat events affecting assets, whether and how the assets are vulnerable to the threats, the likelihood that an asset vulnerability will be exploited by a threat, and the impact (or consequence) of loss of the assets.
As part of the process of selecting security controls for systems, use risk assessments to inform and guide the tailoring process for organizational information systems and environments of operation.
Use risk assessments to inform and guide plan of action and milestones (POA&M) prioritization. Organizations implement a consistent process for developing POA&Ms that uses a prioritized approach to risk mitigation that is uniform across the organization. A risk assessment guides the prioritization process for items included in the plan of action and milestones.

[1] NIST SP 800-37.

Use risk determinations to inform and guide decisions about the operation and use of systems. The authorizing official or designated representative, in collaboration with other security and privacy officials, analyzes the information in the authorization package provided by the control assessor, system owner, or common control provider, and finalizes the determination of risk.

Source: GAO analysis of National Institute of Standards and Technology guidance. | GAO-19-384

Most of the 23 civilian Chief Financial Officers Act agencies addressed the majority of the key practices for incorporating risk-based decision-making in their policies and procedures. However, most of the agencies also had gaps in one or more of these areas. Specifically, six agencies addressed all the elements in their policies and procedures, and the remaining 17 were missing at least one. Table 10 provides details on our assessment of the agencies' policies.

Table 10: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies' Policies and Procedures Addressed Elements to Facilitate Risk-Based Decisions

Agency	Assign roles	Agency-wide risk assessment	Identification of common controls	Control monitoring strategy	System-level risk assessments	Risk assessments for control tailoring	Risk assessments for POA&M[a] prioritization	Risk determinations for system operation
Agriculture	Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Not Addressed	Addressed
Commerce	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed
Education	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
Energy	Addressed	Not Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
HHS	Addressed	Not Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed	Addressed
DHS	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
HUD	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed
Interior	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
Justice	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
Labor	Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Not Addressed	Addressed
State	Addressed	Not Addressed	Addressed	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Addressed
Transportation	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
Treasury	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
VA	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed

Agency	Assign roles	Agency-wide risk assessment	Identification of common controls	Control monitoring strategy	System-level risk assessments	Risk assessments for control tailoring	Risk assessments for POA&M[a] prioritization	Risk determinations for system operation
USAID	Addressed	Not Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed	Addressed
EPA	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
GSA	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
NASA	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed
NSF	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed
NRC	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed
OPM	Addressed	Not Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed	Addressed
SBA	Addressed	Not Addressed	Addressed	Addressed	Addressed	Addressed	Not Addressed	Addressed
SSA	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed	Addressed

Source: GAO analysis of agency policies. | GAO-19-384

Note: Agency abbreviations: Agriculture = Department of Agriculture, Commerce = Department of Commerce, Education = Department of Education, Energy = Department of Energy, HHS = Department of Health and Human Services, DHS = Department of Homeland Security, Interior = Department of the Interior, Justice = Department of Justice, Labor = Department of Labor, State = Department of State, Transportation = Department of Transportation, Treasury = Department of the Treasury, VA = Department of Veterans Affairs, USAID = United States Agency for International Development, EPA = Environmental Protection Agency, GSA = General Services Administration, NASA = National Aeronautics and Space Administration, NSF = National Science Foundation, NRC = Nuclear Regulatory Commission, OPM = Office of Personnel Management, SBA = Small Business Administration, and SSA = Social Security Administration.

[a] Plan of action and milestones

Appendix V: Details on the Extent to Which Agencies Developed an Organization-Wide Cybersecurity Risk Assessment

Of the 23 civilian Chief Financial Officers Act agencies, 12 developed a process for an agency-wide cybersecurity risk assessment. Specifically, these agencies developed processes for aggregating system-level data and analyzing them to assess overall cybersecurity risk to agency operations and assets. The remaining 11 agencies did not establish such a process. Table 11 provides details on our assessment.

Table 11: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Conducted an Agency-Wide Cybersecurity Risk Assessment

Agency	Assessment	Discussion
Department of Agriculture	Met	The Department of Agriculture aggregates cybersecurity risk information from each of its components by producing a bi-weekly cybersecurity scorecard. This scorecard provides an agency-wide view and assessments of key indicators, such as authorization to operate percentages, plan of action and milestones status, and critical vulnerabilities. The report includes a score for each component and for the department as a whole. An Agriculture Security Operations official stated that the scorecard helps determine the component agencies' security posture regarding how they identify and manage vulnerabilities in their endpoints and servers and vulnerability scans and reports are collected on a regular (near-real-time) basis. The information is rolled up into the department's enterprise-level dashboard. Subcomponents have access to the dashboard and are trained to use the enterprise-level tool to gather vulnerability information and remediate vulnerabilities.
Department of Commerce	Not met	Department of Commerce Office of the Chief Information Officer (CIO) officials noted that they are considering options for an enterprise-wide tool with a dashboard capability that can aggregate data from various sources across the department. They stated that this capability would be part of the implementation of the Continuous Diagnostics and Mitigation (CDM) tools from the Department of Homeland Security (DHS).

Agency	Assessment	Discussion
Department of Education	Met	The Department of Education developed a Cybersecurity Framework Risk Scorecard to provide an aggregated view of information system risks across the organization. This process includes risk assessments of individual systems rolled up to the principal office level, organized in terms of the five functions from the National Institute of Standards and Technology's (NIST) cybersecurity framework. These data are used to develop a risk likelihood/impact matrix and a summary of risks for all the department's components. The department uses this process to prioritize areas for remediation, and officials stated that it enabled them to significantly reduce their risk over the course of a year.
Department of Energy	Met	The Department of Energy developed an annual internal controls assessment process, which involved identifying recurrent control weaknesses and prioritizing a smaller set of high-value, actionable controls to rapidly improve the department's security posture. Through this process, the department was able to identify critical IT/cybersecurity risk statements beginning in fiscal year 2015 and has since begun to monitor those weaknesses along with corporate controls in its financial management assurance tool. Officials stated that this has allowed them to monitor and track remedial actions and impose requirements across component agencies.
Department of Health and Human Services	Not met	Department of Health and Human Services CIO officials noted that they use a variety of dashboards, scorecards, and reports from various data sources to monitor risk; they acknowledged, however, that they had not developed an agency-wide cybersecurity risk assessment based on aggregated data from across the department. They noted that they intend, as part of their implementation of their new security, governance, risk and compliance tool, to enhance risk visibility and reporting at the department level. The officials added that they anticipate increased network visibility with further implementation of DHS's CDM program.
Department of Homeland Security	Met	DHS develops a quarterly cybersecurity status report that contains a threat assessment for all of the organizations within the department. The report contains scorecards that analyze security authorization for all systems, weakness remediation, mandatory personal identity verifications, and other factors that would contribute to a thorough check of DHS's systems. The CIO office also uses a scorecard that addresses obsolete systems, plans of action and milestones, and risk levels. DHS officials stated that they receive a report in relation to the scorecard every year that addresses their information assurance compliance systems. DHS uses this report to identify key indicators and give feedback to component CIOs. DHS uses these data to address Federal Information Security Modernization Act (FISMA) of 2014 requirements and NIST guidance and to inform the packages for authorizing officials.
Department of Housing and Urban Development	Met	The Department of Housing and Urban Development uses an enterprise dashboard to aggregate system-level data and scores the agency's maturity in process areas based on the NIST cybersecurity framework. This includes scores for its program offices and the department as a whole. It also allows the department to identify policies and procedures for the 11 process areas (which include continuous monitoring, incident response, identity and access management, and configuration management, among others) and perform a gap analysis to determine process areas that require policy/process development.
Department of the Interior	Met	The Department of the Interior develops a quarterly cybersecurity briefing that aggregates information across the organization to provide risk, FISMA and inspector general assessment ratings, and top vulnerabilities in internal-facing systems.

Agency	Assessment	Discussion
Department of Justice	Met	According to the department's continuous monitoring strategy, it leverages enterprise-wide solutions, such as an endpoint management tool, for automated asset, secure configuration, and vulnerability management. Using data from the endpoint manager and other tools, the department's Security Posture Dashboard Report system provides a risk score for assets and department components based on a number of factors, including vulnerability patch requirements, configuration management, and software management risk assessments. Scores are calculated using a detailed risk scoring methodology, and data are updated on a daily basis. The dashboard report provides department leadership a synthesized view of its enterprise security posture and component-level security details. The Security Posture Dashboard Report system provides an overall security posture score and scores for more specific areas.
Department of Labor	Met	All risk information for the department's networks is maintained in its enterprise Cyber Security Assessment and Management tool. The department provided a consolidated risk analysis for all the information systems in its inventory, as well as the methodology behind the risk analysis and the overall threat matrix that rolls up the risk management areas of concern for the department's network.
Department of State	Met	The Department of State uses a custom application, referred to as iPost, which uses data from various monitoring tools to produce a single, holistic view of technical vulnerabilities. Each host and user account is scored in multiple categories using a scoring method based on the National Vulnerability Database's scoring system for vulnerabilities, where higher scores mean higher risk. Scores are then aggregated across categories to give a risk score for a host, a site, a region, or the enterprise.
Department of Transportation	Met	The Department of Transportation uses various tools to monitor various metrics, such as plan of action and milestones status, vulnerability status and trends, and security assessment status. In addition, the department provided a series of quarterly briefings that showed scores for various risks across the enterprise, including cyber hygiene vulnerability data, top-five high-risk internet-facing hosts/networks, top risk-based vulnerabilities, compliance with web security requirements, email security requirements, most common and oldest critical vulnerabilities, and a count and scoring of vulnerabilities across the department's components. These data are presented at quarterly department CIO council meetings.
Department of the Treasury	Not met	Department of the Treasury officials acknowledged that they had not developed this capability and stated that they are working to complete this in the future.
Department of Veterans Affairs	Not met	Department of Veterans Affairs Office of Information Technology officials described a process whereby VA risk champions and risk analysts work together to identify, assess, and manage potential enterprise risks. However, they did not provide documentation of this process.
U.S. Agency for International Development	Not met	Agency officials described mechanisms they use to conduct an agency-wide cybersecurity risk assessment process. However, the agency was unable to provide documentation that showed the organization-wide risk assessment based on an aggregation of system-level risk information.
Environmental Protection Agency	Not met	Environmental Protection Agency officials described mechanisms they use to conduct an agency-wide cybersecurity risk assessment process. However, the agency was unable to provide documentation that showed the organization-wide risk assessment based on an aggregation of system-level risk information.
General Services Administration	Not met	General Services Administration CIO officials provided a vulnerability risk report as evidence to support that the agency conducts an agency-wide cybersecurity risk assessment. While its vulnerability risk report does include risks, it is not an aggregate of system-level cybersecurity risks. General Services Administration CIO officials stated that it is the agency's intention to aggregate system-level data as part of its efforts to implement the CDM program.

Agency	Assessment	Discussion
National Aeronautics and Space Administration	Not met	Agency cyber risk officials acknowledged that they had not developed a process for aggregating system-level risks across the agency. They stated that their cyber integration team is responsible for developing an assessment of the agency's capabilities against the NIST cybersecurity framework to provide a view of high-level risks, but that they had not yet developed a process for elevating system-level risks to provide an enterprise-level assessment.
National Science Foundation	Met	The National Science Foundation assesses risks through various methods and produces a quarterly security assessment report that is intended to provide its authorizing officials, Senior Agency Official for Privacy, system owners, Chief Information Security Officer, IT Security Officer, and stakeholders an overview of the IT security program to support decisions regarding the ongoing authorization of the agency's systems.
Nuclear Regulatory Commission	Not met	The Nuclear Regulatory Commission's CIO stated that the agency has a compliance table that they include in their daily reports that looks across the organization and is a tool for describing cyber risks uncovered through various system assessments. The daily report addresses security incidents and upcoming security deployments. However, it does not provide a comprehensive view across the entire organization based on system-level data.
Office of Personnel Management	Not met	Office of Personnel Management officials described mechanisms they use to conduct an agency-wide cybersecurity risk assessment. However, the agency did not provide documentation that showed their organization-wide risk assessment based on an aggregation of system-level risk information.
Small Business Administration	Not met	Small Business Administration officials described mechanisms they use to conduct an agency-wide cybersecurity risk assessment process. However, the agency was unable to provide documentation that showed their organization-wide risk assessment was based on an aggregation of system-level risk information.
Social Security Administration	Met	The Social Security Administration (SSA) established a process for a consolidated cyber risk register that provides an overview of the organizational cyber risk. The register maintains a comprehensive understanding of cybersecurity risks by aggregating all cybersecurity findings, gaps, and vulnerabilities into a centralized report so SSA can gain a single view of cybersecurity risks at an aggregate level. This is to enable consistent reporting and help senior management make informed risk based decisions.

Source: GAO analysis of agency data. | GAO-19-384

Appendix VI: Details on Agencies' Processes for Coordination between Cybersecurity and Enterprise Risk Management

Of the 23 civilian Chief Financial Officers Act agencies, 10 fully established a process or mechanism for coordination between their cybersecurity risk executive and their enterprise risk management (ERM) governance structure, five agencies partially established such a process, and the remaining eight agencies did not provide evidence of coordination. Table 12 provides details on our assessment.

Table 12: Extent to Which the 23 Civilian Chief Financial Officers Act Agencies Established Coordination between Their Cybersecurity Risk Executive and Enterprise Risk Management (ERM) Governance

Agency	Assessment	Discussion
Department of Agriculture	Not met	The United States Department of Agriculture (Agriculture) has not fully established its ERM governance structure and did not provide evidence of coordination with the cybersecurity risk executive. Officials from Agriculture's Office of the Chief Information Officer (CIO) stated that the department does not have an enterprise risk management council, although some agencies within USDA are individually working on their risk profiles. They added that the department has engaged a contractor to develop a proof of concept to better understand its risk environment.
Department of Commerce	Met	The Department of Commerce (Commerce) established and documented a council—the Departmental Management Council—that is responsible for ERM. Within the office of the CIO, Commerce's Office of Cyber Security and IT Risk Management serves as the department's cybersecurity risk executive, and the office of the CIO has representation on the department-wide ERM council. In addition, Commerce has committees and councils that meet regularly to discuss risks associated with the department. These groups include a CIO Council, which is chaired by the Commerce CIO, as well as a committee made up of bureau Chief Information Security Officers and IT Security Officers, which is facilitated by the Commerce Chief Information Security Officer (CISO) and reports to the CIO Council. All high-level information security issues discussed within the CIO Council are briefed to the Departmental Management Council.
Department of Education	Met	The Department of Education's Senior Management Council is responsible for assisting the Deputy Secretary/Chief Operating Officer in providing strategic direction on department operations and management, including the implementation of the department's enterprise risk management. The department's CIO, who serves as the cybersecurity risk executive, sits on this council.

Agency	Assessment	Discussion
Department of Energy	Met	Enterprise risk management for the agency has been incorporated into the department's Internal Controls Program, and its Office of the Chief Financial Officer is responsible for enterprise risk management and internal controls. The Departmental Internal Controls and Audit Review Council is responsible for identifying new areas or issues for senior management discussion and determination for appropriate departmental reporting. The department's Cyber Council serves as the corporate cybersecurity risk executive function; the department's CIO is represented on both the Cyber Council and the enterprise-level risk council.
Department of Health and Human Services	Not met	Officials with the department's CIO office stated that they have an enterprise risk council responsible for managing the department's risks, including updating and maintaining its risk profile and working with risk owners to develop responses to priority risks. However, these officials did not provide documentation of the department's enterprise risk management governance structure or evidence of coordination between this entity and the cybersecurity risk executive.
Department of Homeland Security	Not met	The Department of Homeland Security established and fully documented its enterprise risk management governance structure and cybersecurity risk executive function and stated that coordination occurs between these functions. However, the department did not provide evidence or specific details of this coordination.
Department of Housing and Urban Development	Met	The agency established the Executive Risk Management Council, which is composed of senior leaders from various offices to provide governance of enterprise risk management. The council includes the department's CIO in its membership, who also serves as the department's cybersecurity risk executive.
Department of the Interior	Not met	The department has not fully established an enterprise risk management governance structure or an approach to coordination with cybersecurity risk management. The department's Deputy CIO stated that the department is still in the process of developing such a governance structure. He also noted that the department had carried out a pilot project to test an approach to enterprise risk management, which yielded useful information for future efforts.
Department of Justice	Partially met	The department incorporated enterprise risk management into its Strategic Objective Review process, which is to be facilitated by its Office of Strategic Planning and Performance, and created the position of Director of Strategic Planning and Performance with responsibilities related to enterprise risk management. In addition, the department provided evidence that its CIO and CISO attended meetings of its Senior Assessment Team, which included discussion of enterprise risk management. However, the department has not fully defined or documented its enterprise risk management process, including how coordination with the cybersecurity risk executive is to occur.
Department of Labor	Met	The department's Senior Enterprise Risk Management Team oversees the risk management activities carried out by component organizations to ensure effective risk-based decisions and approves risks at the enterprise level. The department's CIO and CISO are both members of this team, and the CIO is the department's cybersecurity risk executive.
Department of State	Not met	The Department of State established an enterprise risk management governance structure and cybersecurity risk executive function and stated that coordination occurs between these functions. However, the department did not provide evidence or specific details of this coordination.
Department of Transportation	Partially met	The department provided evidence that its Deputy CIO was involved in the department's performance management review, which officials from the Office of the Chief Financial Officer described as the process they use for ERM, as coordinated by the Office of the Chief Financial Officer; however, the department has not fully documented this process, including coordination with the department's cybersecurity risk executive.

Agency	Assessment	Discussion
Department of the Treasury	Not met	The Department of the Treasury established an enterprise risk management governance structure and cybersecurity risk executive function and officials stated that coordination occurs between these functions. However, the department did not provide evidence or specific details of this coordination.
Department of Veterans Affairs	Not met	The department did not provide documentation of its ERM function or of coordination with its cybersecurity risk executive. Office of Information and Technology officials stated that they have an agency-wide risk management group and that coordination takes place between this group and the cybersecurity risk executive; however, they did not provide documentation of this group or specific details showing coordination.
U.S. Agency for International Development	Met	The agency assigned its Executive Management Council on Risk and Internal Control with responsibility for the agency's enterprise risk management function. The agency's CISO, who is the risk executive for cybersecurity, regularly attends meetings with the council to discuss cybersecurity risk issues.
Environmental Protection Agency	Partially met	According to agency officials, the agency's Office of the Chief Financial Officer and a group responsible for enterprise risks meets on a regular basis to discuss enterprise risks. In addition, the agency's CIO, Chief Operating Officer, and Deputy Administrator are all involved in those meetings and information security risks are discussed. However, the agency has not fully documented its enterprise risk management governance structure and coordination process.
General Services Administration	Partially met	The agency has assigned responsibilities for enterprise risk management to its Investment Review Board, and this board includes the agency's CIO as a member and co-chair. However, as previously noted, the General Services Administration has not formally documented the position or responsibilities of the cybersecurity risk executive in its policy and thus could not show that the risk executive was involved in enterprise risk management activities.
National Aeronautics and Space Administration	Met	The National Aeronautics and Space Administration's (NASA) Executive Council serves as its senior decision-making body and its highest governing council. The Agency Program Management Council is a subordinate council of the Executive Council and is responsible for, among other things, risk management and risk acceptance for the National Aeronautics and Space Administration (NASA). Although NASA's Senior Agency Information Security Officer, who is the agency's cyber risk executive, is not a member of the Program Management Council, the CIO is represented on the council and the agency provided evidence of regular communication between the Senior Agency Information Security Officer and CIO.
National Science Foundation	Met	The National Science Foundation assigned an existing governance structure responsibility for enterprise risk management, which is composed of the agency's Director, Chief Operating Officer, assistant directors and directors, who convene via a "round table" to address agency-wide risks. The agency's CIO, who is the risk executive for cybersecurity, reports directly to the agency Chief Operating Officer regarding cybersecurity risks to be discussed at the round table.
Nuclear Regulatory Commission	Not met	The Nuclear Regulatory Commission established an enterprise risk management governance structure and cybersecurity risk executive function and stated that coordination occurs between these functions. However, the agency did not provide evidence or specific details of this coordination.
Office of Personnel Management	Met	The agency established a risk management council, chaired by the Chief Management Officer and including members from each of its main business organizations (including the CIO and CISO). The council's responsibilities include establishing a program to identify, assess, measure, and manage the major risks facing the agency. The agency's CISO is responsible for cybersecurity risk and also serves as a member of the risk management council.
Small Business Administration	Met	The agency has an enterprise risk management board at the senior executive level that considers risks affecting the entire organization. The board comprises senior leaders from major agency offices including, among others, the CIO, who serves as the agency's cybersecurity risk executive.

Agency	Assessment	Discussion
Social Security Administration	Partially met	The agency provided an email related to the development of the agency's enterprise risk profile, which included the CISO. However, the agency has not formally defined or documented its ERM process, including coordination with the cybersecurity risk executive function.

Source: GAO analysis of agency data. | GAO-19-384

Appendix VII: Recommendations to Departments and Agencies

We are making a total of 57 recommendations to the 23 civilian *Chief Financial Officers Act* agencies in our review to fully address key practices in their cybersecurity risk management policies and procedures.

The Secretary of Agriculture should take the following three actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 2)
- Update the department's policies to require (1) the use of risk assessments to inform security control tailoring and (2) the use of risk assessments to inform plan of actions and milestones (POA&M) prioritization. (Recommendation 3)
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 4)

The Secretary of Commerce should take the following two actions:

- Update the department's policies to require (1) an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform POA&M prioritization. (Recommendation 5)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 6)

The Secretary of Education should take the following action:

- Fully develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 7)

The Secretary of Energy should take the following two actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 8)

- Update the department’s policies to require (1) an organization-wide cybersecurity risk assessment and (2) the identification of common controls. (Recommendation 9)

The Secretary of Health and Human Services should take the following four actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 10)
- Update the department’s policies to require (1) an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform security control tailoring. (Recommendation 11)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 12)
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 13)

The Secretary of Homeland Security should take the following two actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 14)
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 15)

The Secretary of Housing and Urban Developing should take the following two actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 16)
- Update the department’s policies to require the use of risk assessments to inform POA&M prioritization. (Recommendation 17)

The Secretary of the Interior should take the following three actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 18)
- Update the department’s policies to require an organization-wide cybersecurity risk assessment. (Recommendation 19)

- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 20)

The Attorney General should take the following two actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 21)
- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 22)

The Secretary of Labor should take the following action:

- Update the department’s policies to require (1) the use of risk assessments to inform control tailoring and (2) the use of risk assessments to inform POA&M prioritization. (Recommendation 23)

The Secretary of State should take the following two actions:

- 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 POA&M prioritization. (Recommendation 24)
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 25)

The Secretary of Transportation should take the following three actions:

- Fully develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 26)
- Update the department’s policies to require an organization-wide risk assessment. (Recommendation 27)
- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 28)

The Secretary of the Treasury should take the following three actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 29)

- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 30)
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 31)

The Secretary of Veterans Affairs should take the following four actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 32)
- Update the department's policies to require an organization-wide cybersecurity risk assessment. (Recommendation 33)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 34)
- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 35)

The Administrator of USAID should take the following two actions:

- Update the agency's policies to require (1) an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform control tailoring. (Recommendation 36)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 37)

The Administrator of EPA should take the following four actions:

- Fully develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 38)
- Update the agency's policies to require an organization-wide cybersecurity risk assessment. (Recommendation 39)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 40)
- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 41)

The Administrator of General Services should take the following four actions:

- Designate and document a risk executive function with responsibilities for organization-wide cybersecurity risk management. (Recommendation 42)
- Update the agency's policies to require an organization-wide cybersecurity risk assessment. (Recommendation 43)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 44)
- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 45)

The Administrator of NASA should take the following two actions:

- Update the agency's policies to require (1) an organization-wide risk assessment and (2) the use of risk assessments to inform POA&M prioritization. (Recommendation 46)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 47)

We are not making a recommendation to NASA to establish a cybersecurity risk management strategy because we previously made such a recommendation, which remains open.[1]

The Director of NSF should take the following action:

- Fully develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 48)

The Chairman of NRC should take the following four actions:

- Develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 49)
- Update the agency's policies to require (1) an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform POA&M prioritization. (Recommendation 50)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 51)

[1] GAO, *NASA Information Technology: Urgent Action Needed to Address Significant Management and Cybersecurity Weaknesses*, GAO-18-337 (Washington, D.C.: May 2018).

- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 52)

The Director of OPM should take the following two actions:

- Update the agency’s policies to require (1) an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform control tailoring. (Recommendation 53)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 54)

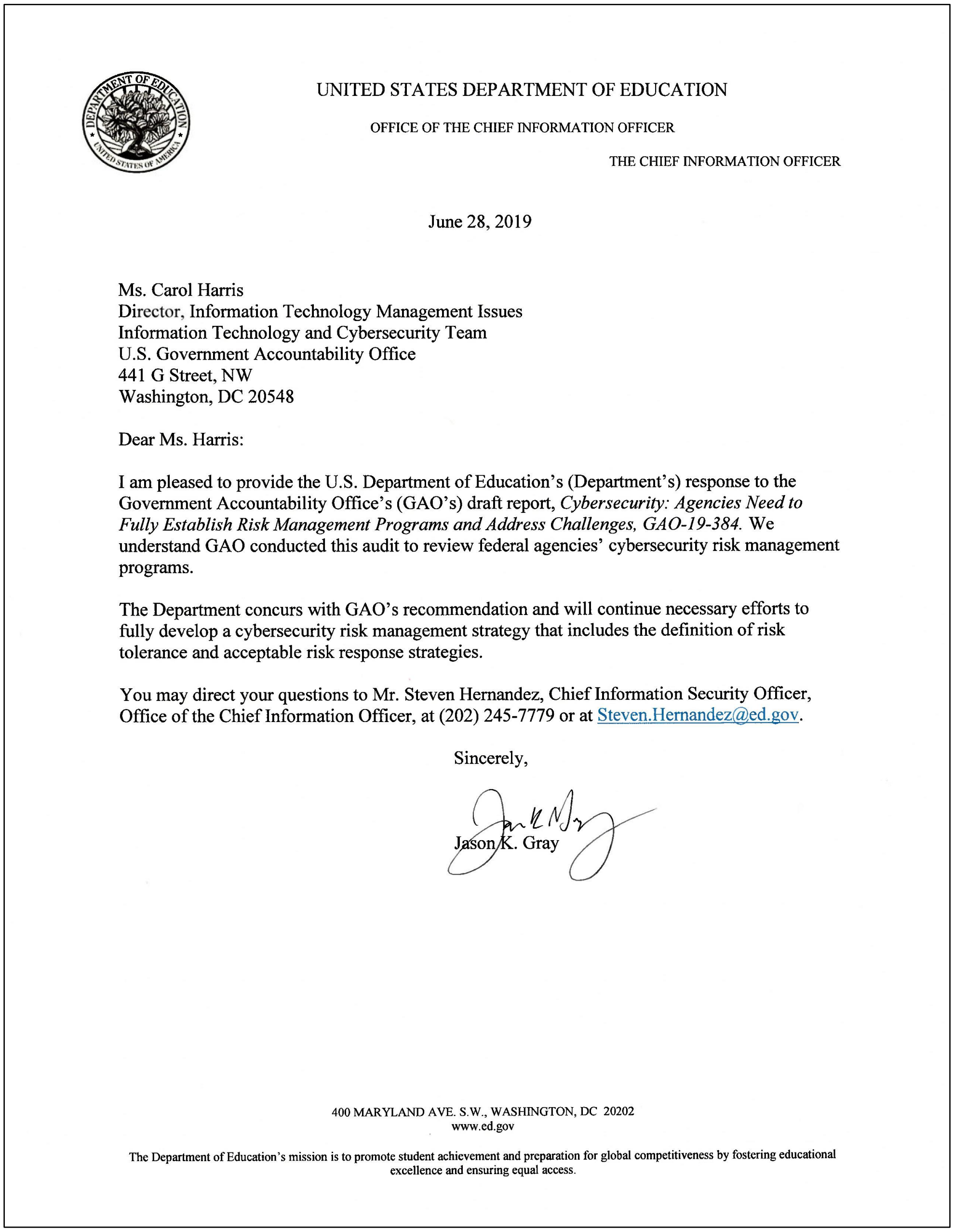
The Administrator of SBA should take the following three actions:

- Fully develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Recommendation 55)
- Update the agency’s policies to require (1) an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform POA&M prioritization. (Recommendation 56)
- Establish a process for conducting an organization-wide cybersecurity risk assessment. (Recommendation 57)

The Commissioner of SSA should take the following action:

- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (Recommendation 58)

Appendix VIII: Comments from the Department of Education



UNITED STATES DEPARTMENT OF EDUCATION

OFFICE OF THE CHIEF INFORMATION OFFICER

THE CHIEF INFORMATION OFFICER

June 28, 2019

Ms. Carol Harris
Director, Information Technology Management Issues
Information Technology and Cybersecurity Team
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

I am pleased to provide the U.S. Department of Education's (Department's) response to the Government Accountability Office's (GAO's) draft report, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges, GAO-19-384.* We understand GAO conducted this audit to review federal agencies' cybersecurity risk management programs.

The Department concurs with GAO's recommendation and will continue necessary efforts to fully develop a cybersecurity risk management strategy that includes the definition of risk tolerance and acceptable risk response strategies.

You may direct your questions to Mr. Steven Hernandez, Chief Information Security Officer, Office of the Chief Information Officer, at (202) 245-7779 or at Steven.Hernandez@ed.gov.

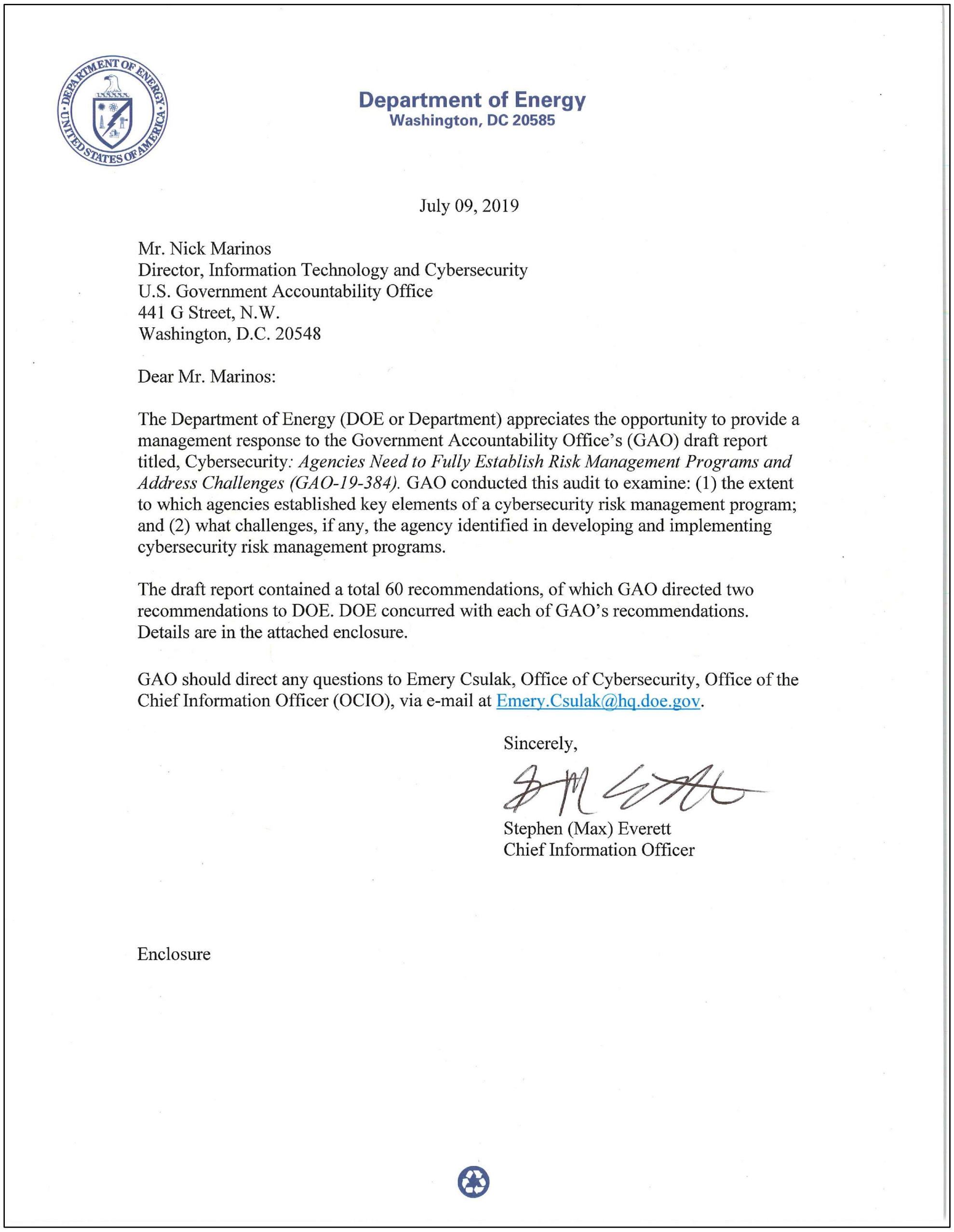
Sincerely,

Jason K. Gray

400 MARYLAND AVE. S.W., WASHINGTON, DC 20202
www.ed.gov

The Department of Education's mission is to promote student achievement and preparation for global competitiveness by fostering educational excellence and ensuring equal access.

Appendix IX: Comments from the Department of Energy



Department of Energy
Washington, DC 20585

July 09, 2019

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Marinos:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a management response to the Government Accountability Office's (GAO) draft report titled, Cybersecurity*: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384).* GAO conducted this audit to examine: (1) the extent to which agencies established key elements of a cybersecurity risk management program; and (2) what challenges, if any, the agency identified in developing and implementing cybersecurity risk management programs.

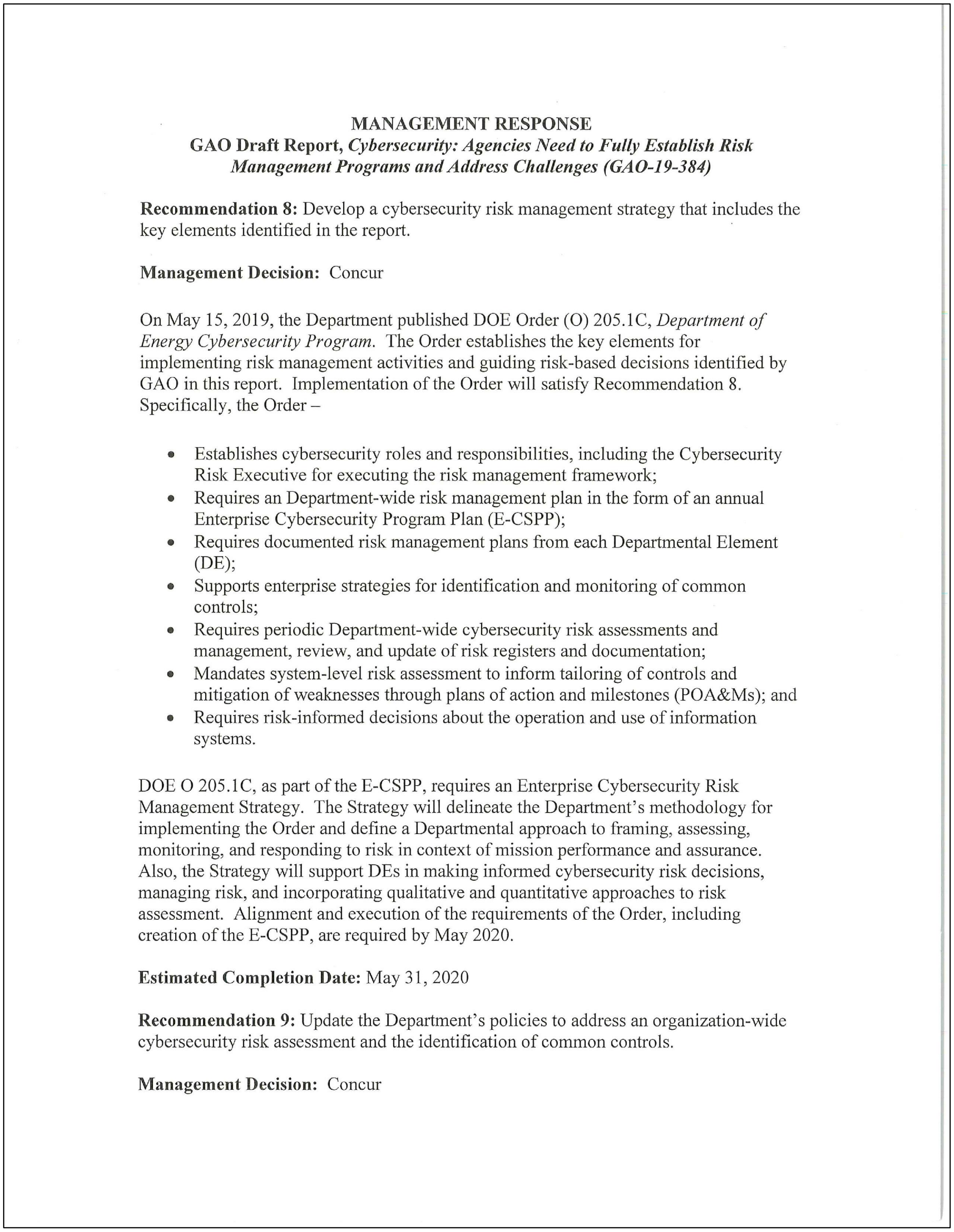
The draft report contained a total 60 recommendations, of which GAO directed two recommendations to DOE. DOE concurred with each of GAO's recommendations. Details are in the attached enclosure.

GAO should direct any questions to Emery Csulak, Office of Cybersecurity, Office of the Chief Information Officer (OCIO), via e-mail at Emery.Csulak@hq.doe.gov.

Sincerely,

Stephen (Max) Everett
Chief Information Officer

Enclosure



MANAGEMENT RESPONSE
GAO Draft Report, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384)*

Recommendation 8: Develop a cybersecurity risk management strategy that includes the key elements identified in the report.

Management Decision: Concur

On May 15, 2019, the Department published DOE Order (O) 205.1C, *Department of Energy Cybersecurity Program*. The Order establishes the key elements for implementing risk management activities and guiding risk-based decisions identified by GAO in this report. Implementation of the Order will satisfy Recommendation 8. Specifically, the Order –

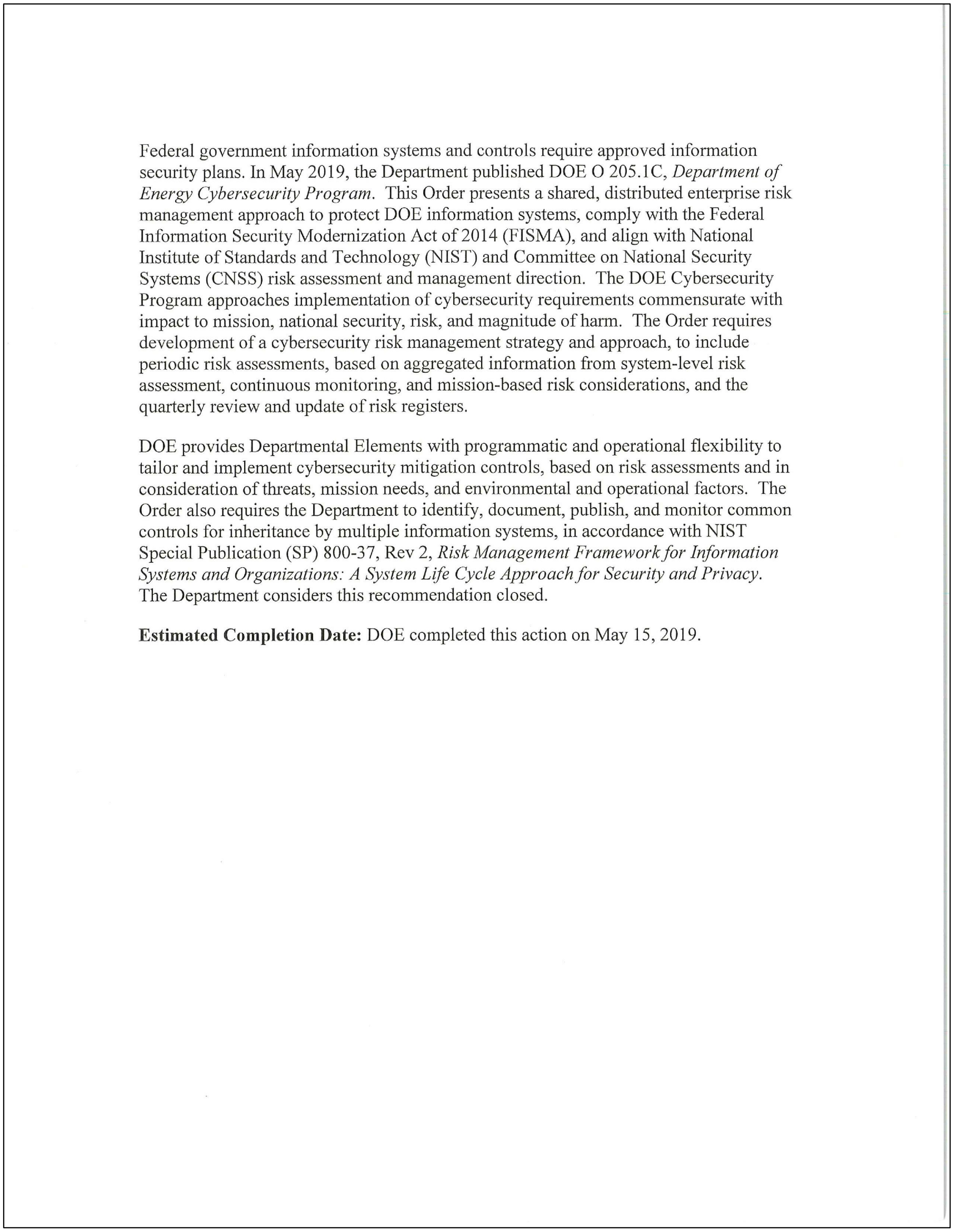
- Establishes cybersecurity roles and responsibilities, including the Cybersecurity Risk Executive for executing the risk management framework;
- Requires an Department-wide risk management plan in the form of an annual Enterprise Cybersecurity Program Plan (E-CSPP);
- Requires documented risk management plans from each Departmental Element (DE);
- Supports enterprise strategies for identification and monitoring of common controls;
- Requires periodic Department-wide cybersecurity risk assessments and management, review, and update of risk registers and documentation;
- Mandates system-level risk assessment to inform tailoring of controls and mitigation of weaknesses through plans of action and milestones (POA&Ms); and
- Requires risk-informed decisions about the operation and use of information systems.

DOE O 205.1C, as part of the E-CSPP, requires an Enterprise Cybersecurity Risk Management Strategy. The Strategy will delineate the Department's methodology for implementing the Order and define a Departmental approach to framing, assessing, monitoring, and responding to risk in context of mission performance and assurance. Also, the Strategy will support DEs in making informed cybersecurity risk decisions, managing risk, and incorporating qualitative and quantitative approaches to risk assessment. Alignment and execution of the requirements of the Order, including creation of the E-CSPP, are required by May 2020.

Estimated Completion Date: May 31, 2020

Recommendation 9: Update the Department's policies to address an organization-wide cybersecurity risk assessment and the identification of common controls.

Management Decision: Concur

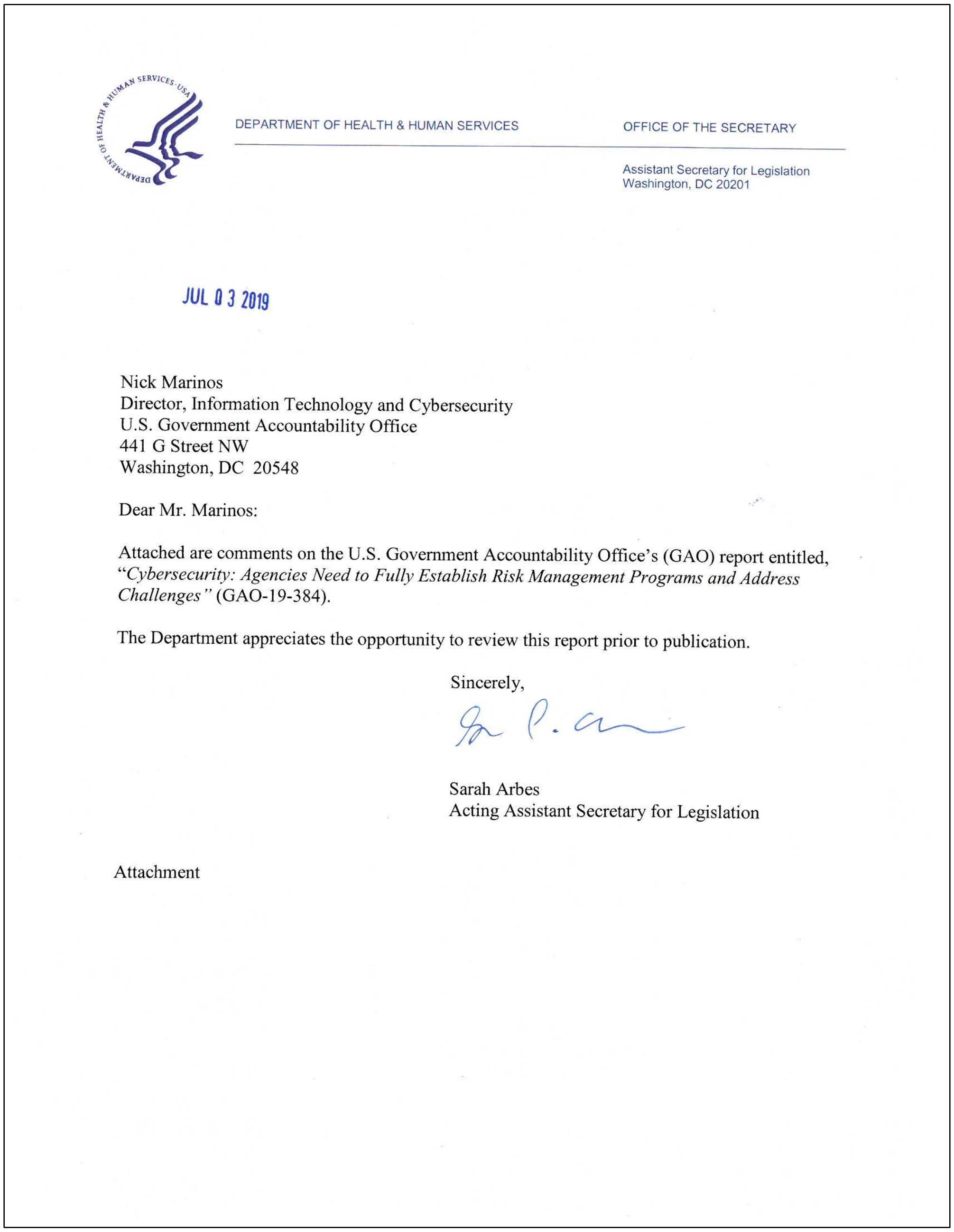


Federal government information systems and controls require approved information security plans. In May 2019, the Department published DOE O 205.1C, *Department of Energy Cybersecurity Program*. This Order presents a shared, distributed enterprise risk management approach to protect DOE information systems, comply with the Federal Information Security Modernization Act of 2014 (FISMA), and align with National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) risk assessment and management direction. The DOE Cybersecurity Program approaches implementation of cybersecurity requirements commensurate with impact to mission, national security, risk, and magnitude of harm. The Order requires development of a cybersecurity risk management strategy and approach, to include periodic risk assessments, based on aggregated information from system-level risk assessment, continuous monitoring, and mission-based risk considerations, and the quarterly review and update of risk registers.

DOE provides Departmental Elements with programmatic and operational flexibility to tailor and implement cybersecurity mitigation controls, based on risk assessments and in consideration of threats, mission needs, and environmental and operational factors. The Order also requires the Department to identify, document, publish, and monitor common controls for inheritance by multiple information systems, in accordance with NIST Special Publication (SP) 800-37, Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. The Department considers this recommendation closed.

Estimated Completion Date: DOE completed this action on May 15, 2019.

Appendix X: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

JUL 0 3 2019

Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Marinos:

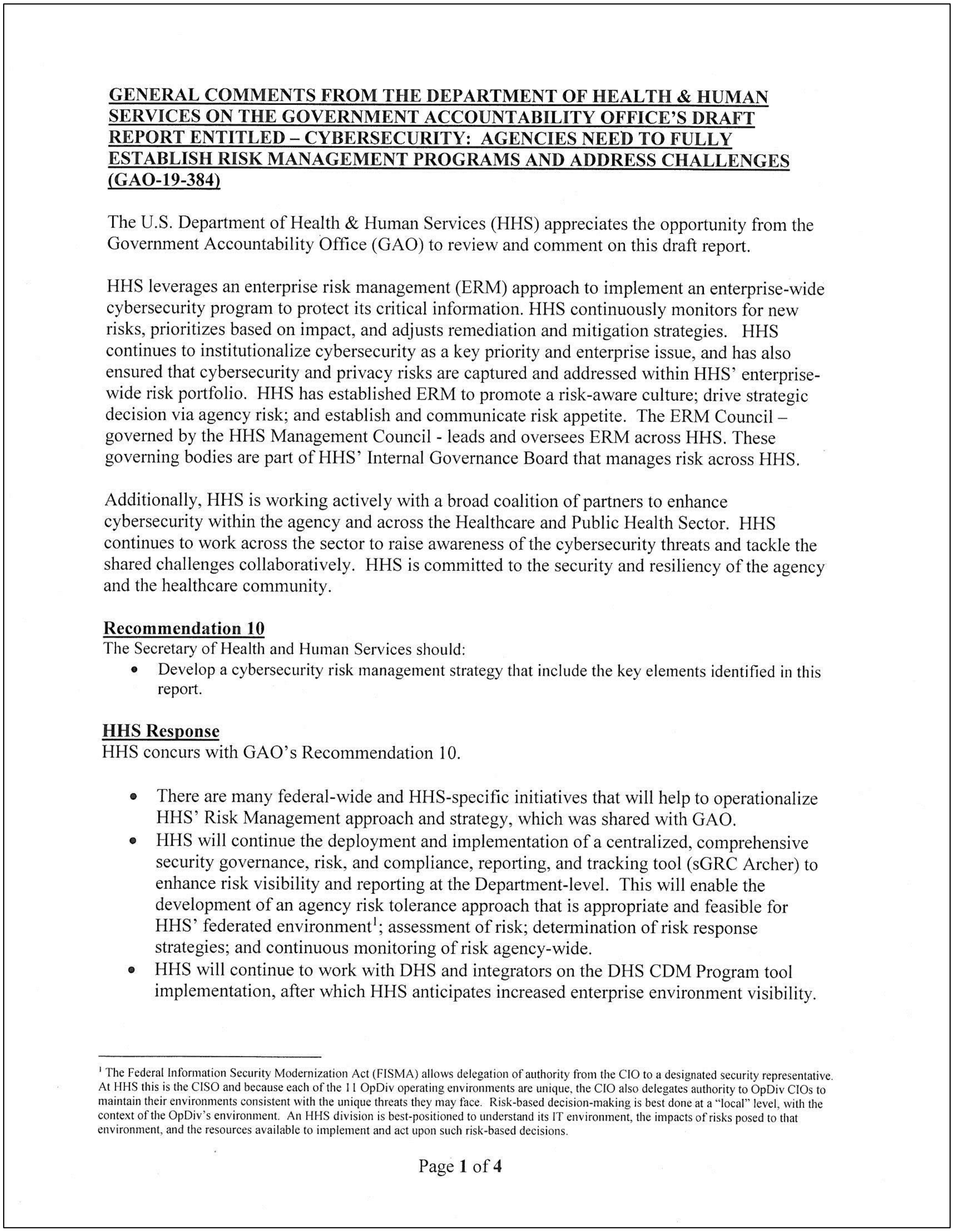
Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "*Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*" (GAO-19-384).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Sarah Arbes
Acting Assistant Secretary for Legislation

Attachment



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED – CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES (GAO-19-384)

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

HHS leverages an enterprise risk management (ERM) approach to implement an enterprise-wide cybersecurity program to protect its critical information. HHS continuously monitors for new risks, prioritizes based on impact, and adjusts remediation and mitigation strategies. HHS continues to institutionalize cybersecurity as a key priority and enterprise issue, and has also ensured that cybersecurity and privacy risks are captured and addressed within HHS' enterprise-wide risk portfolio. HHS has established ERM to promote a risk-aware culture; drive strategic decision via agency risk; and establish and communicate risk appetite. The ERM Council – governed by the HHS Management Council - leads and oversees ERM across HHS. These governing bodies are part of HHS' Internal Governance Board that manages risk across HHS.

Additionally, HHS is working actively with a broad coalition of partners to enhance cybersecurity within the agency and across the Healthcare and Public Health Sector. HHS continues to work across the sector to raise awareness of the cybersecurity threats and tackle the shared challenges collaboratively. HHS is committed to the security and resiliency of the agency and the healthcare community.

Recommendation 10

The Secretary of Health and Human Services should:

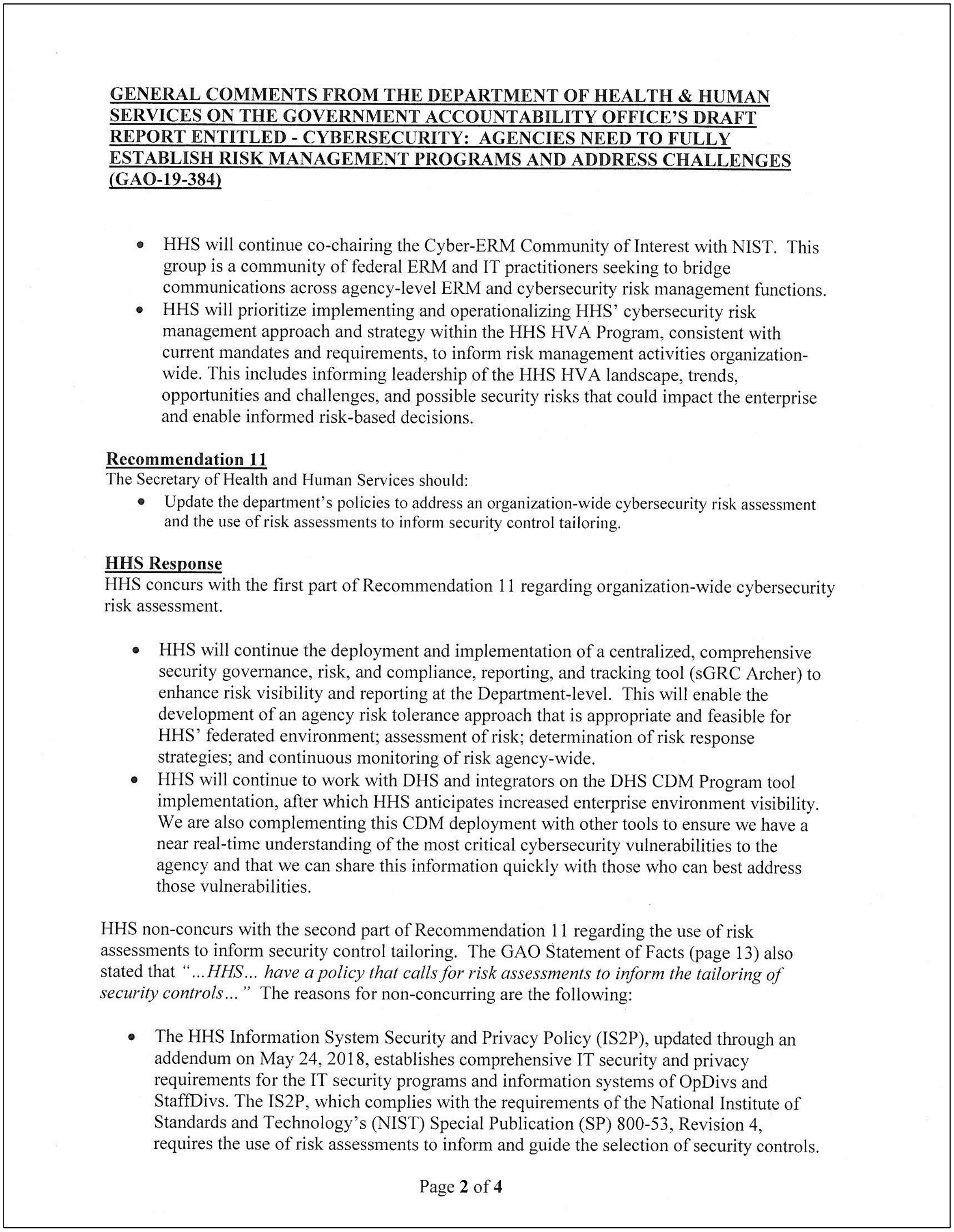
- Develop a cybersecurity risk management strategy that include the key elements identified in this report.

HHS Response

HHS concurs with GAO's Recommendation 10.

- There are many federal-wide and HHS-specific initiatives that will help to operationalize HHS' Risk Management approach and strategy, which was shared with GAO.
- HHS will continue the deployment and implementation of a centralized, comprehensive security governance, risk, and compliance, reporting, and tracking tool (sGRC Archer) to enhance risk visibility and reporting at the Department-level. This will enable the development of an agency risk tolerance approach that is appropriate and feasible for HHS' federated environment[1]; assessment of risk; determination of risk response strategies; and continuous monitoring of risk agency-wide.
- HHS will continue to work with DHS and integrators on the DHS CDM Program tool implementation, after which HHS anticipates increased enterprise environment visibility.

[1] The Federal Information Security Modernization Act (FISMA) allows delegation of authority from the CIO to a designated security representative. At HHS this is the CISO and because each of the 11 OpDiv operating environments are unique, the CIO also delegates authority to OpDiv CIOs to maintain their environments consistent with the unique threats they may face. Risk-based decision-making is best done at a "local" level, with the context of the OpDiv's environment. An HHS division is best-positioned to understand its IT environment, the impacts of risks posed to that environment, and the resources available to implement and act upon such risk-based decisions.



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES (GAO-19-384)

- HHS will continue co-chairing the Cyber-ERM Community of Interest with NIST. This group is a community of federal ERM and IT practitioners seeking to bridge communications across agency-level ERM and cybersecurity risk management functions.
- HHS will prioritize implementing and operationalizing HHS' cybersecurity risk management approach and strategy within the HHS HVA Program, consistent with current mandates and requirements, to inform risk management activities organization-wide. This includes informing leadership of the HHS HVA landscape, trends, opportunities and challenges, and possible security risks that could impact the enterprise and enable informed risk-based decisions.

Recommendation 11

The Secretary of Health and Human Services should:

- Update the department's policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform security control tailoring.

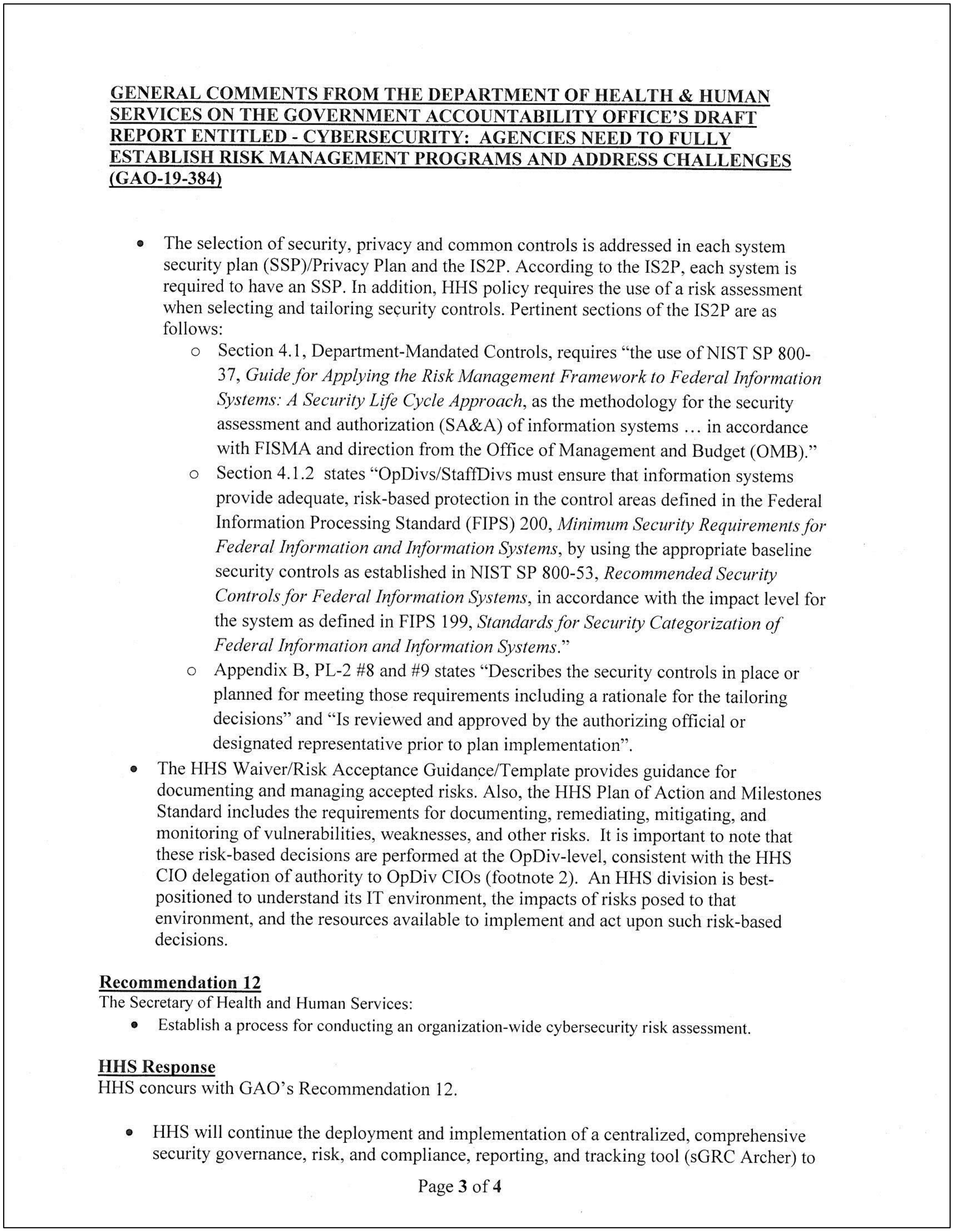
HHS Response

HHS concurs with the first part of Recommendation 11 regarding organization-wide cybersecurity risk assessment.

- HHS will continue the deployment and implementation of a centralized, comprehensive security governance, risk, and compliance, reporting, and tracking tool (sGRC Archer) to enhance risk visibility and reporting at the Department-level. This will enable the development of an agency risk tolerance approach that is appropriate and feasible for HHS' federated environment; assessment of risk; determination of risk response strategies; and continuous monitoring of risk agency-wide.
- HHS will continue to work with DHS and integrators on the DHS CDM Program tool implementation, after which HHS anticipates increased enterprise environment visibility. We are also complementing this CDM deployment with other tools to ensure we have a near real-time understanding of the most critical cybersecurity vulnerabilities to the agency and that we can share this information quickly with those who can best address those vulnerabilities.

HHS non-concurs with the second part of Recommendation 11 regarding the use of risk assessments to inform security control tailoring. The GAO Statement of Facts (page 13) also stated that *"...HHS... have a policy that calls for risk assessments to inform the tailoring of security controls..."* The reasons for non-concurring are the following:

- The HHS Information System Security and Privacy Policy (IS2P), updated through an addendum on May 24, 2018, establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of OpDivs and StaffDivs. The IS2P, which complies with the requirements of the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, requires the use of risk assessments to inform and guide the selection of security controls.



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES (GAO-19-384)

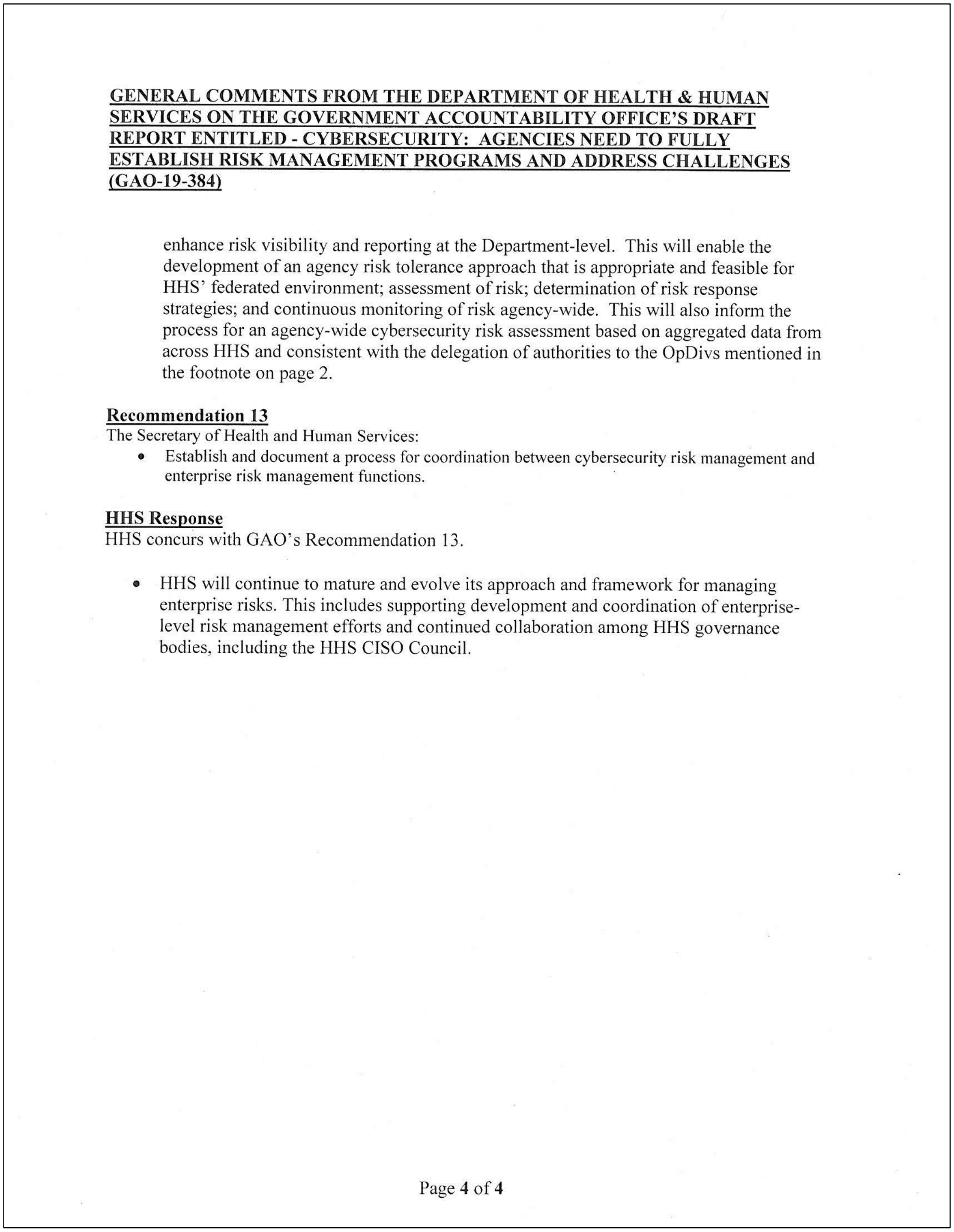
- The selection of security, privacy and common controls is addressed in each system security plan (SSP)/Privacy Plan and the IS2P. According to the IS2P, each system is required to have an SSP. In addition, HHS policy requires the use of a risk assessment when selecting and tailoring security controls. Pertinent sections of the IS2P are as follows:
    - Section 4.1, Department-Mandated Controls, requires "the use of NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, as the methodology for the security assessment and authorization (SA&A) of information systems … in accordance with FISMA and direction from the Office of Management and Budget (OMB)."
    - Section 4.1.2 states "OpDivs/StaffDivs must ensure that information systems provide adequate, risk-based protection in the control areas defined in the Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*, by using the appropriate baseline security controls as established in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, in accordance with the impact level for the system as defined in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*."
    - Appendix B, PL-2 #8 and #9 states "Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions" and "Is reviewed and approved by the authorizing official or designated representative prior to plan implementation".
- The HHS Waiver/Risk Acceptance Guidance/Template provides guidance for documenting and managing accepted risks. Also, the HHS Plan of Action and Milestones Standard includes the requirements for documenting, remediating, mitigating, and monitoring of vulnerabilities, weaknesses, and other risks. It is important to note that these risk-based decisions are performed at the OpDiv-level, consistent with the HHS CIO delegation of authority to OpDiv CIOs (footnote 2). An HHS division is best-positioned to understand its IT environment, the impacts of risks posed to that environment, and the resources available to implement and act upon such risk-based decisions.

Recommendation 12
The Secretary of Health and Human Services:

- Establish a process for conducting an organization-wide cybersecurity risk assessment.

HHS Response
HHS concurs with GAO's Recommendation 12.

- HHS will continue the deployment and implementation of a centralized, comprehensive security governance, risk, and compliance, reporting, and tracking tool (sGRC Archer) to



GENERAL COMMENTS FROM THE DEPARTMENT OF HEALTH & HUMAN SERVICES ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S DRAFT REPORT ENTITLED - CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES (GAO-19-384)

enhance risk visibility and reporting at the Department-level. This will enable the development of an agency risk tolerance approach that is appropriate and feasible for HHS' federated environment; assessment of risk; determination of risk response strategies; and continuous monitoring of risk agency-wide. This will also inform the process for an agency-wide cybersecurity risk assessment based on aggregated data from across HHS and consistent with the delegation of authorities to the OpDivs mentioned in the footnote on page 2.

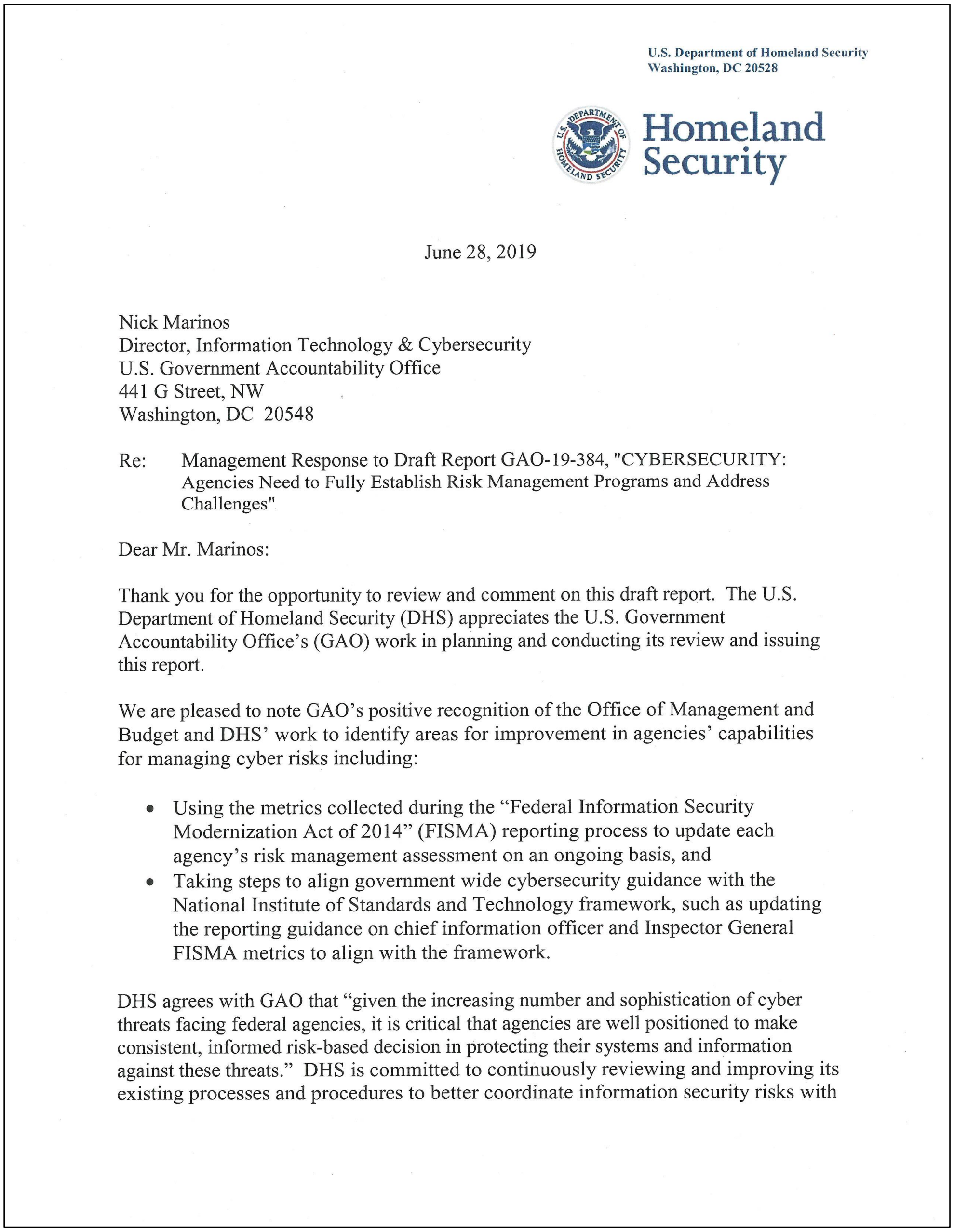
Recommendation 13
The Secretary of Health and Human Services:

- Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

HHS Response
HHS concurs with GAO's Recommendation 13.

- HHS will continue to mature and evolve its approach and framework for managing enterprise risks. This includes supporting development and coordination of enterprise-level risk management efforts and continued collaboration among HHS governance bodies, including the HHS CISO Council.

Appendix XI: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

June 28, 2019

Nick Marinos
Director, Information Technology & Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-384, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges"

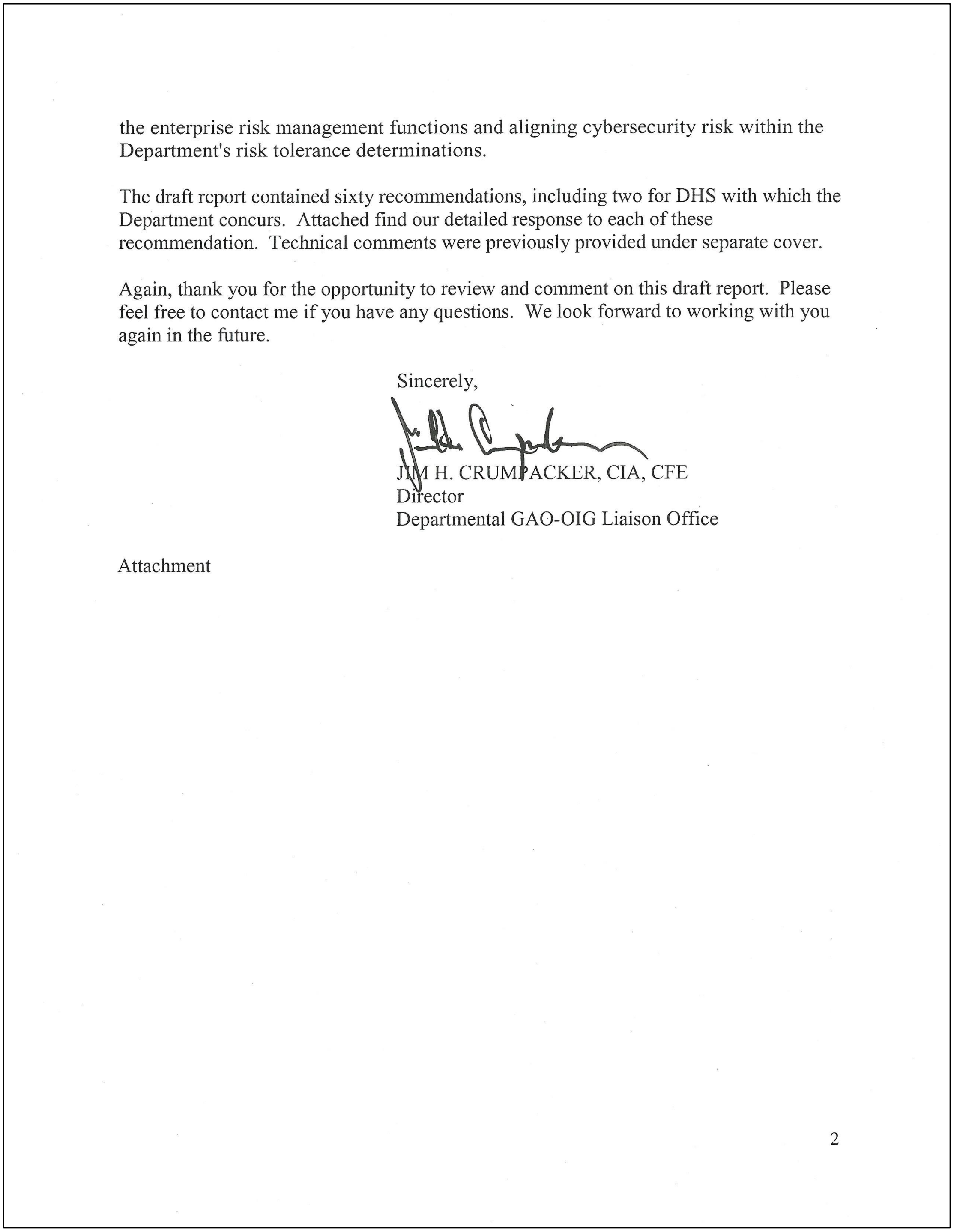
Dear Mr. Marinos:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

We are pleased to note GAO's positive recognition of the Office of Management and Budget and DHS' work to identify areas for improvement in agencies' capabilities for managing cyber risks including:

- Using the metrics collected during the "Federal Information Security Modernization Act of 2014" (FISMA) reporting process to update each agency's risk management assessment on an ongoing basis, and
- Taking steps to align government wide cybersecurity guidance with the National Institute of Standards and Technology framework, such as updating the reporting guidance on chief information officer and Inspector General FISMA metrics to align with the framework.

DHS agrees with GAO that "given the increasing number and sophistication of cyber threats facing federal agencies, it is critical that agencies are well positioned to make consistent, informed risk-based decision in protecting their systems and information against these threats." DHS is committed to continuously reviewing and improving its existing processes and procedures to better coordinate information security risks with



the enterprise risk management functions and aligning cybersecurity risk within the Department's risk tolerance determinations.

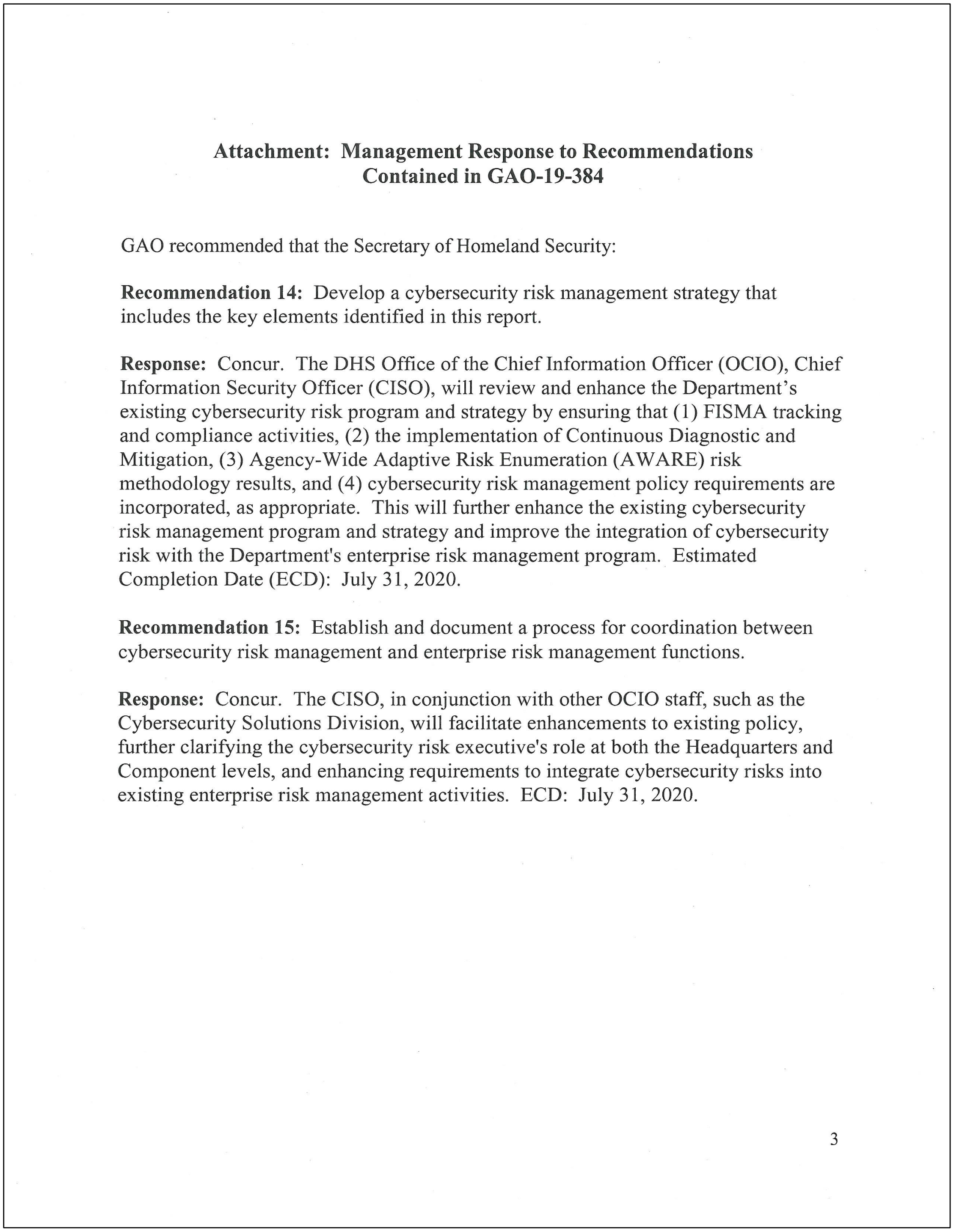
The draft report contained sixty recommendations, including two for DHS with which the Department concurs. Attached find our detailed response to each of these recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment



Attachment: Management Response to Recommendations Contained in GAO-19-384

GAO recommended that the Secretary of Homeland Security:

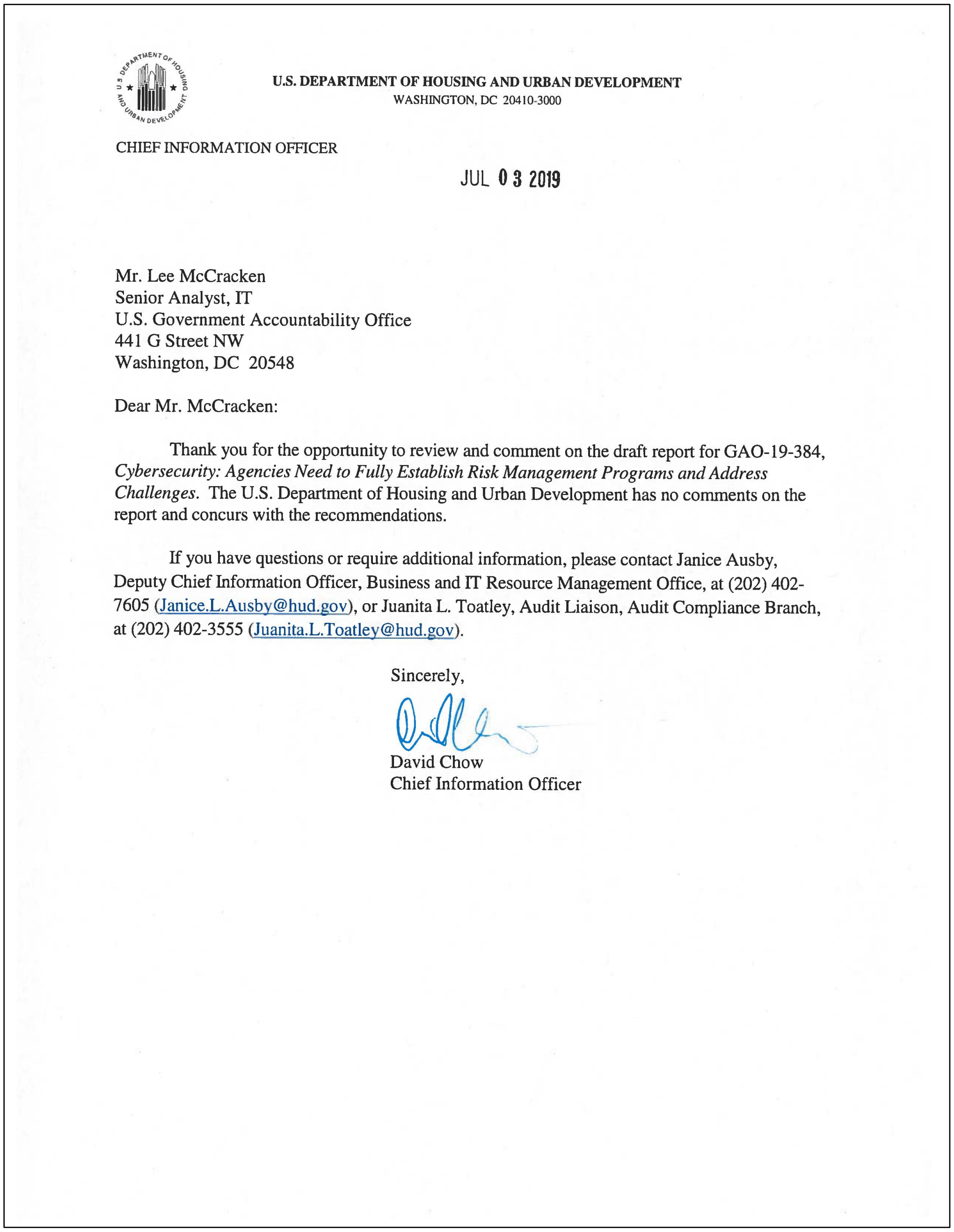
Recommendation 14: Develop a cybersecurity risk management strategy that includes the key elements identified in this report.

Response: Concur. The DHS Office of the Chief Information Officer (OCIO), Chief Information Security Officer (CISO), will review and enhance the Department's existing cybersecurity risk program and strategy by ensuring that (1) FISMA tracking and compliance activities, (2) the implementation of Continuous Diagnostic and Mitigation, (3) Agency-Wide Adaptive Risk Enumeration (AWARE) risk methodology results, and (4) cybersecurity risk management policy requirements are incorporated, as appropriate. This will further enhance the existing cybersecurity risk management program and strategy and improve the integration of cybersecurity risk with the Department's enterprise risk management program. Estimated Completion Date (ECD): July 31, 2020.

Recommendation 15: Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Response: Concur. The CISO, in conjunction with other OCIO staff, such as the Cybersecurity Solutions Division, will facilitate enhancements to existing policy, further clarifying the cybersecurity risk executive's role at both the Headquarters and Component levels, and enhancing requirements to integrate cybersecurity risks into existing enterprise risk management activities. ECD: July 31, 2020.

Appendix XII: Comments from the Department of Housing and Urban Development



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, DC 20410-3000

CHIEF INFORMATION OFFICER

JUL 03 2019

Mr. Lee McCracken
Senior Analyst, IT
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

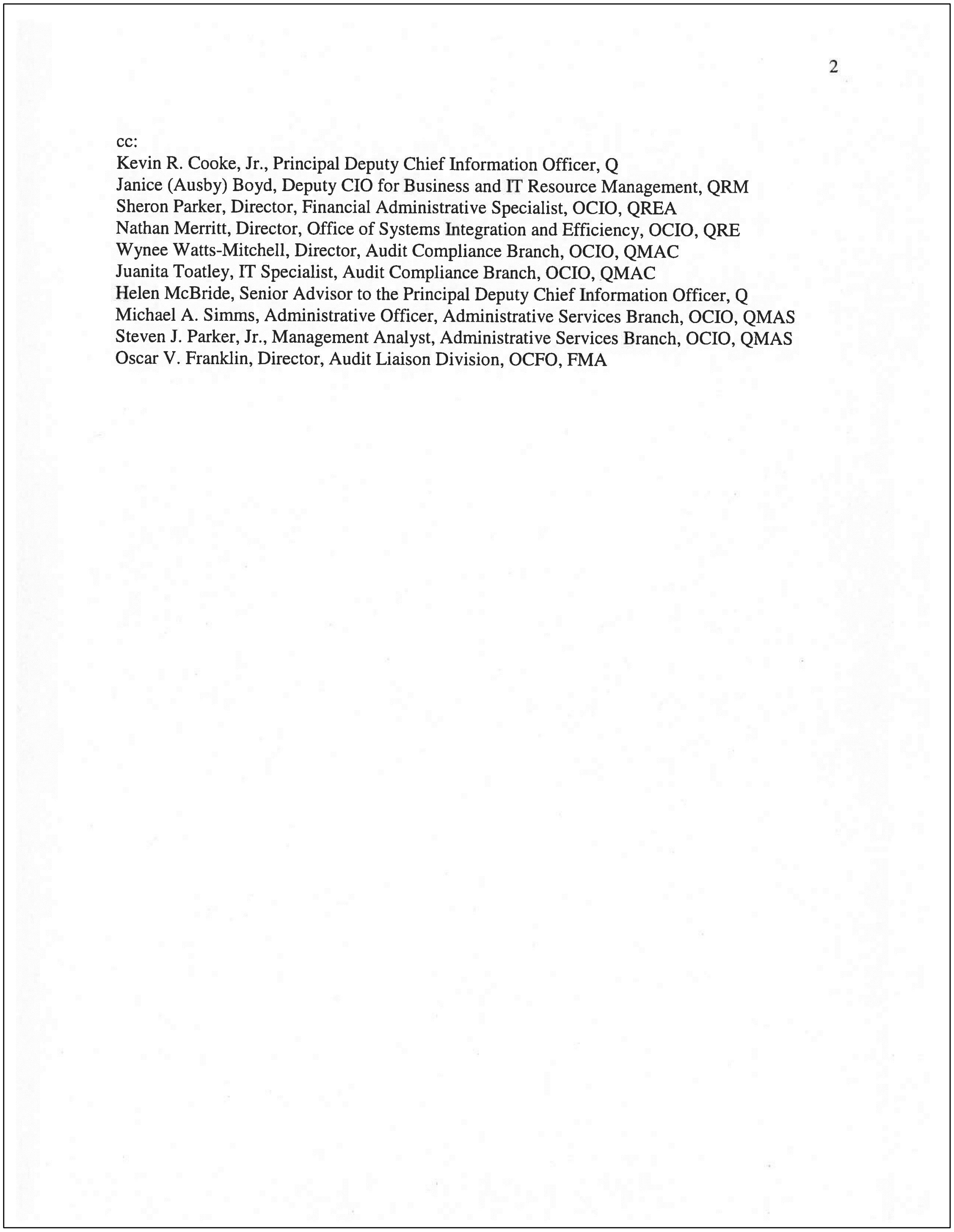
Dear Mr. McCracken:

Thank you for the opportunity to review and comment on the draft report for GAO-19-384, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*. The U.S. Department of Housing and Urban Development has no comments on the report and concurs with the recommendations.

If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 (Janice.L.Ausby@hud.gov), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.gov).

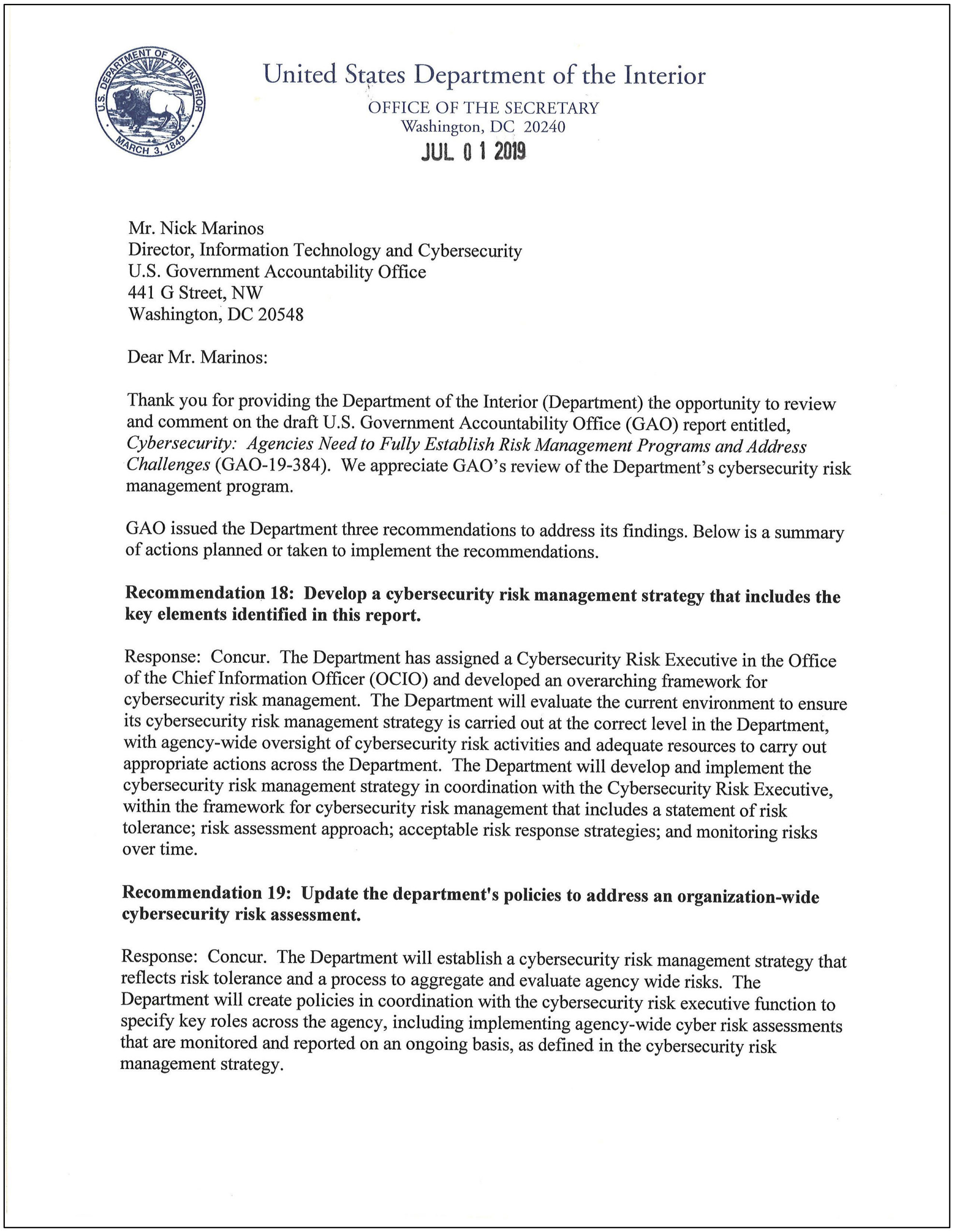
Sincerely,

David Chow
Chief Information Officer



cc:
Kevin R. Cooke, Jr., Principal Deputy Chief Information Officer, Q
Janice (Ausby) Boyd, Deputy CIO for Business and IT Resource Management, QRM
Sheron Parker, Director, Financial Administrative Specialist, OCIO, QREA
Nathan Merritt, Director, Office of Systems Integration and Efficiency, OCIO, QRE
Wynee Watts-Mitchell, Director, Audit Compliance Branch, OCIO, QMAC
Juanita Toatley, IT Specialist, Audit Compliance Branch, OCIO, QMAC
Helen McBride, Senior Advisor to the Principal Deputy Chief Information Officer, Q
Michael A. Simms, Administrative Officer, Administrative Services Branch, OCIO, QMAS
Steven J. Parker, Jr., Management Analyst, Administrative Services Branch, OCIO, QMAS
Oscar V. Franklin, Director, Audit Liaison Division, OCFO, FMA

Appendix XIII: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

JUL 0 1 2019

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

Thank you for providing the Department of the Interior (Department) the opportunity to review and comment on the draft U.S. Government Accountability Office (GAO) report entitled, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges* (GAO-19-384). We appreciate GAO's review of the Department's cybersecurity risk management program.

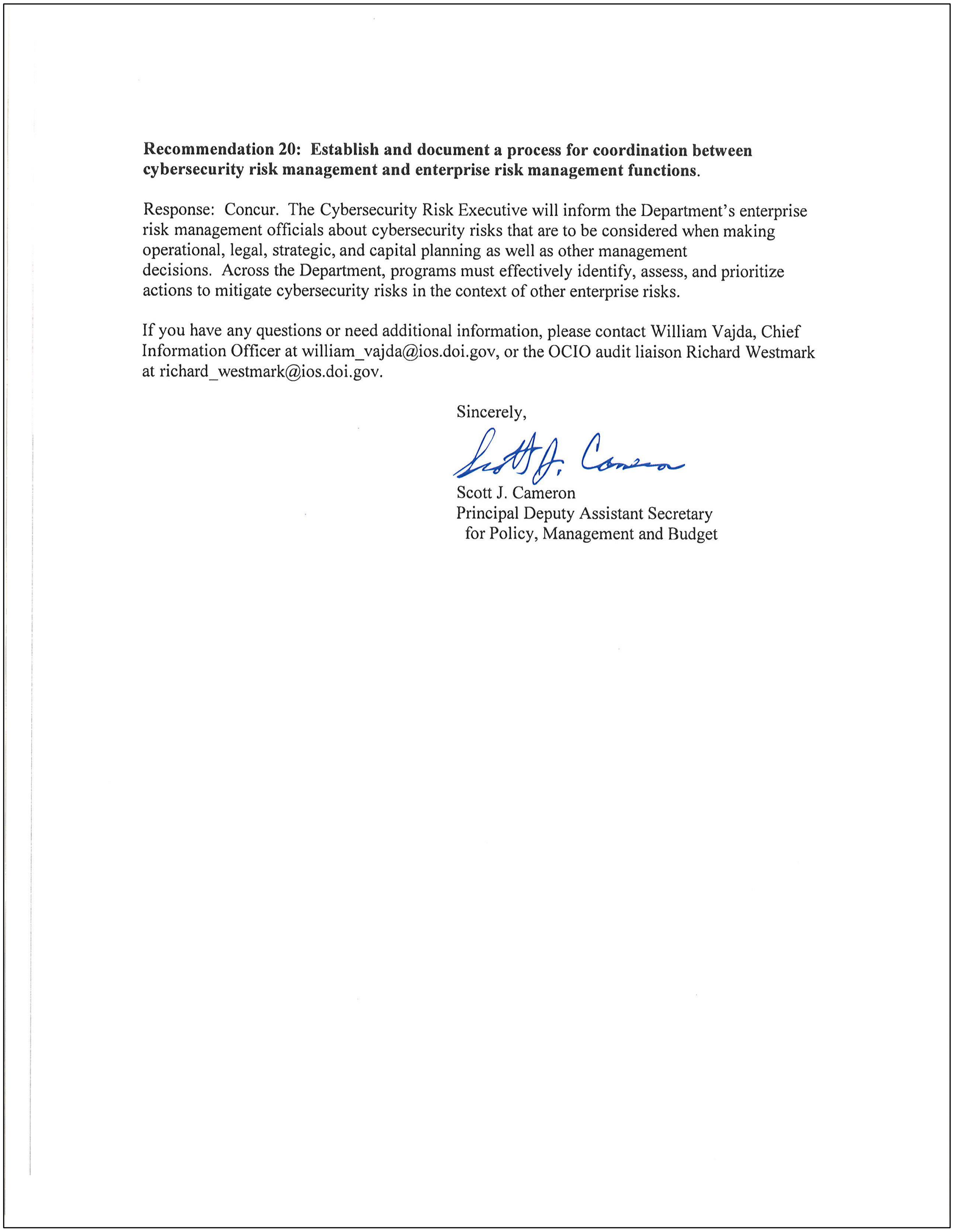
GAO issued the Department three recommendations to address its findings. Below is a summary of actions planned or taken to implement the recommendations.

Recommendation 18: Develop a cybersecurity risk management strategy that includes the key elements identified in this report.

Response: Concur. The Department has assigned a Cybersecurity Risk Executive in the Office of the Chief Information Officer (OCIO) and developed an overarching framework for cybersecurity risk management. The Department will evaluate the current environment to ensure its cybersecurity risk management strategy is carried out at the correct level in the Department, with agency-wide oversight of cybersecurity risk activities and adequate resources to carry out appropriate actions across the Department. The Department will develop and implement the cybersecurity risk management strategy in coordination with the Cybersecurity Risk Executive, within the framework for cybersecurity risk management that includes a statement of risk tolerance; risk assessment approach; acceptable risk response strategies; and monitoring risks over time.

Recommendation 19: Update the department's policies to address an organization-wide cybersecurity risk assessment.

Response: Concur. The Department will establish a cybersecurity risk management strategy that reflects risk tolerance and a process to aggregate and evaluate agency wide risks. The Department will create policies in coordination with the cybersecurity risk executive function to specify key roles across the agency, including implementing agency-wide cyber risk assessments that are monitored and reported on an ongoing basis, as defined in the cybersecurity risk management strategy.



Recommendation 20: Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Response: Concur. The Cybersecurity Risk Executive will inform the Department's enterprise risk management officials about cybersecurity risks that are to be considered when making operational, legal, strategic, and capital planning as well as other management decisions. Across the Department, programs must effectively identify, assess, and prioritize actions to mitigate cybersecurity risks in the context of other enterprise risks.

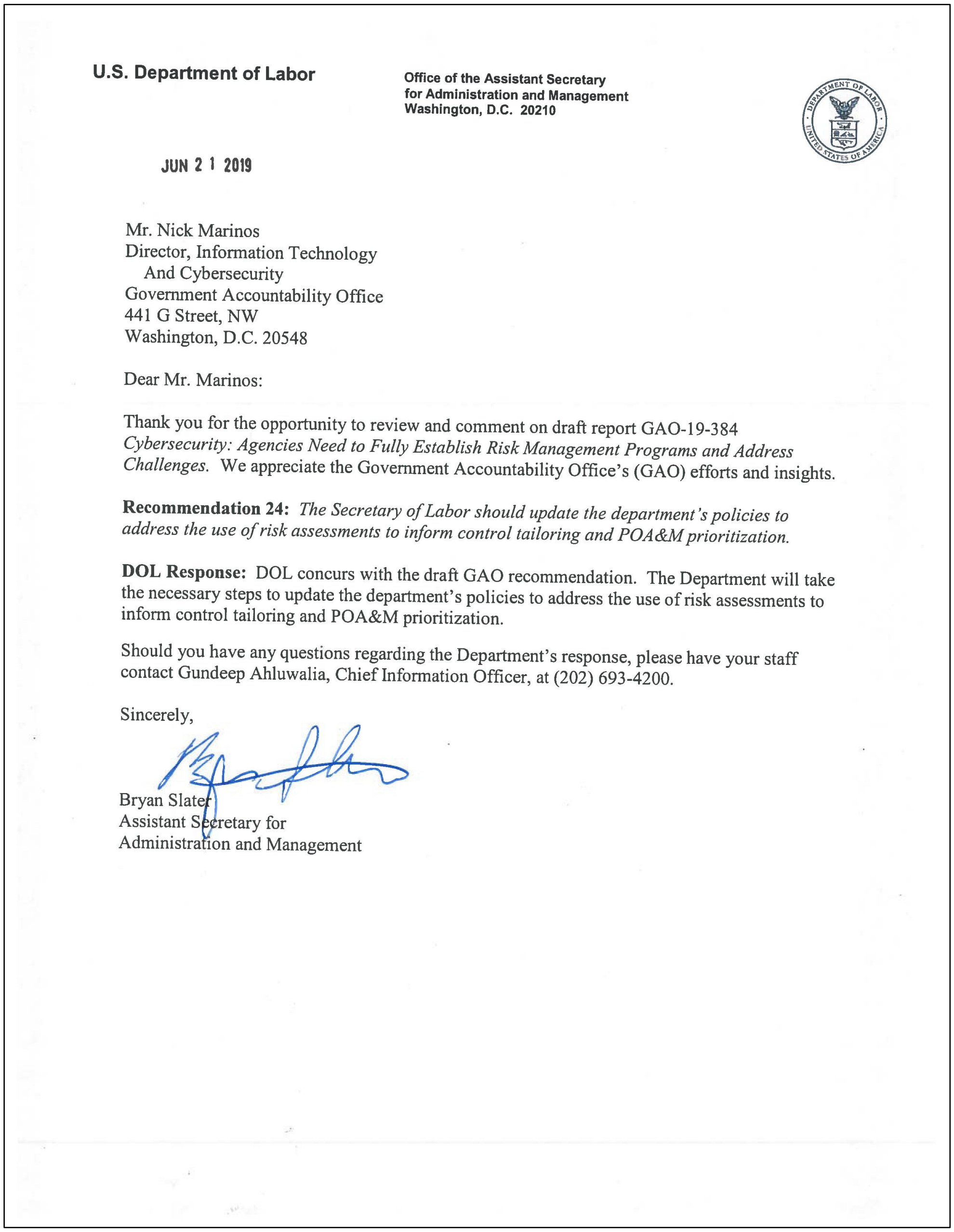
If you have any questions or need additional information, please contact William Vajda, Chief Information Officer at william_vajda@ios.doi.gov, or the OCIO audit liaison Richard Westmark at richard_westmark@ios.doi.gov.

Sincerely,

Scott J. Cameron

Scott J. Cameron
Principal Deputy Assistant Secretary
for Policy, Management and Budget

Appendix XIV: Comments from the Department of Labor



U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210

JUN 2 1 2019

Mr. Nick Marinos
Director, Information Technology
And Cybersecurity
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for the opportunity to review and comment on draft report GAO-19-384 *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges.* We appreciate the Government Accountability Office's (GAO) efforts and insights.

Recommendation 24: *The Secretary of Labor should update the department's policies to address the use of risk assessments to inform control tailoring and POA&M prioritization.*

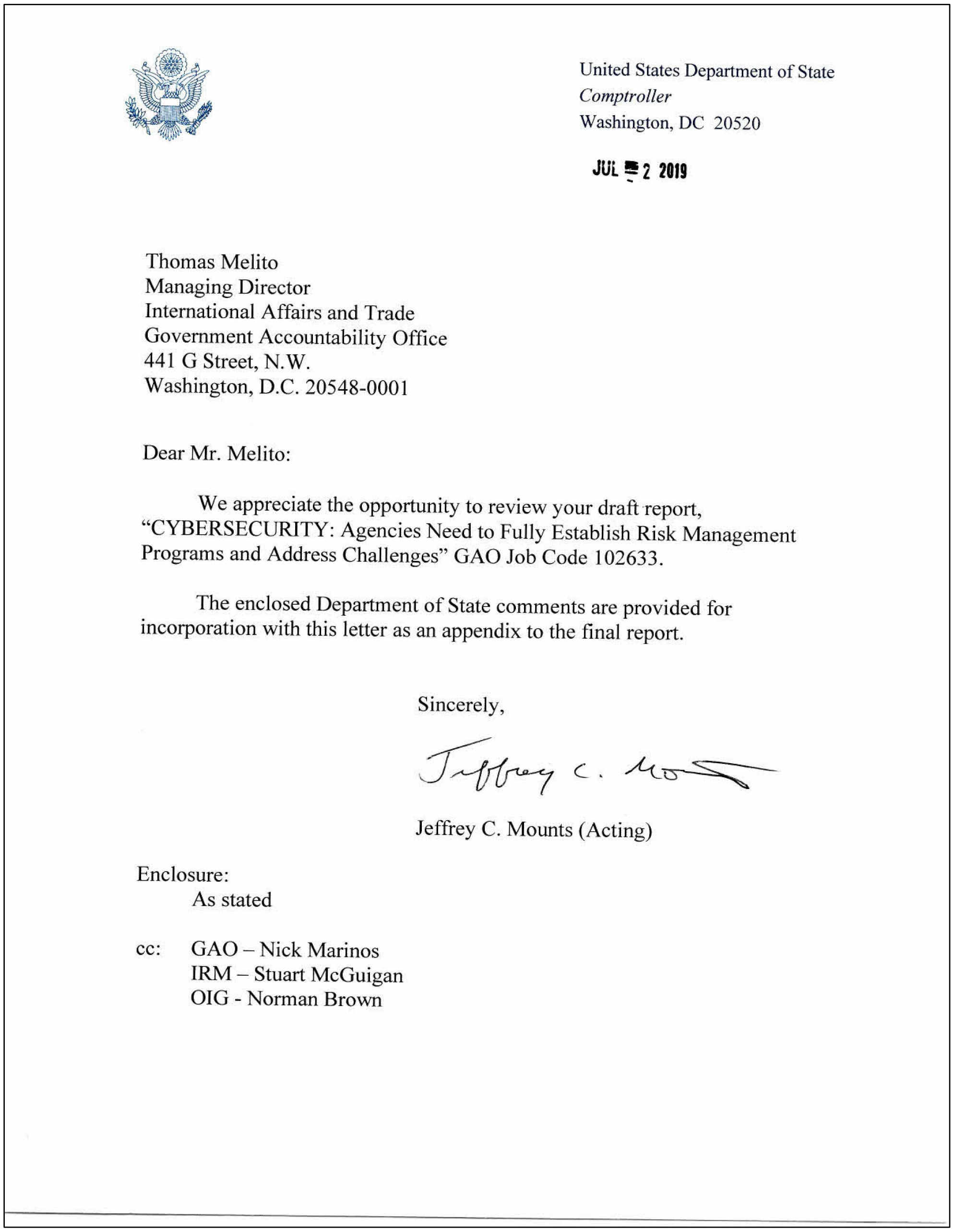
DOL Response: DOL concurs with the draft GAO recommendation. The Department will take the necessary steps to update the department's policies to address the use of risk assessments to inform control tailoring and POA&M prioritization.

Should you have any questions regarding the Department's response, please have your staff contact Gundeep Ahluwalia, Chief Information Officer, at (202) 693-4200.

Sincerely,

Bryan Slater
Assistant Secretary for
Administration and Management

Appendix XV: Comments from the Department of State



United States Department of State
Comptroller
Washington, DC 20520

JUL 2 2019

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

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges" GAO Job Code 102633.

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

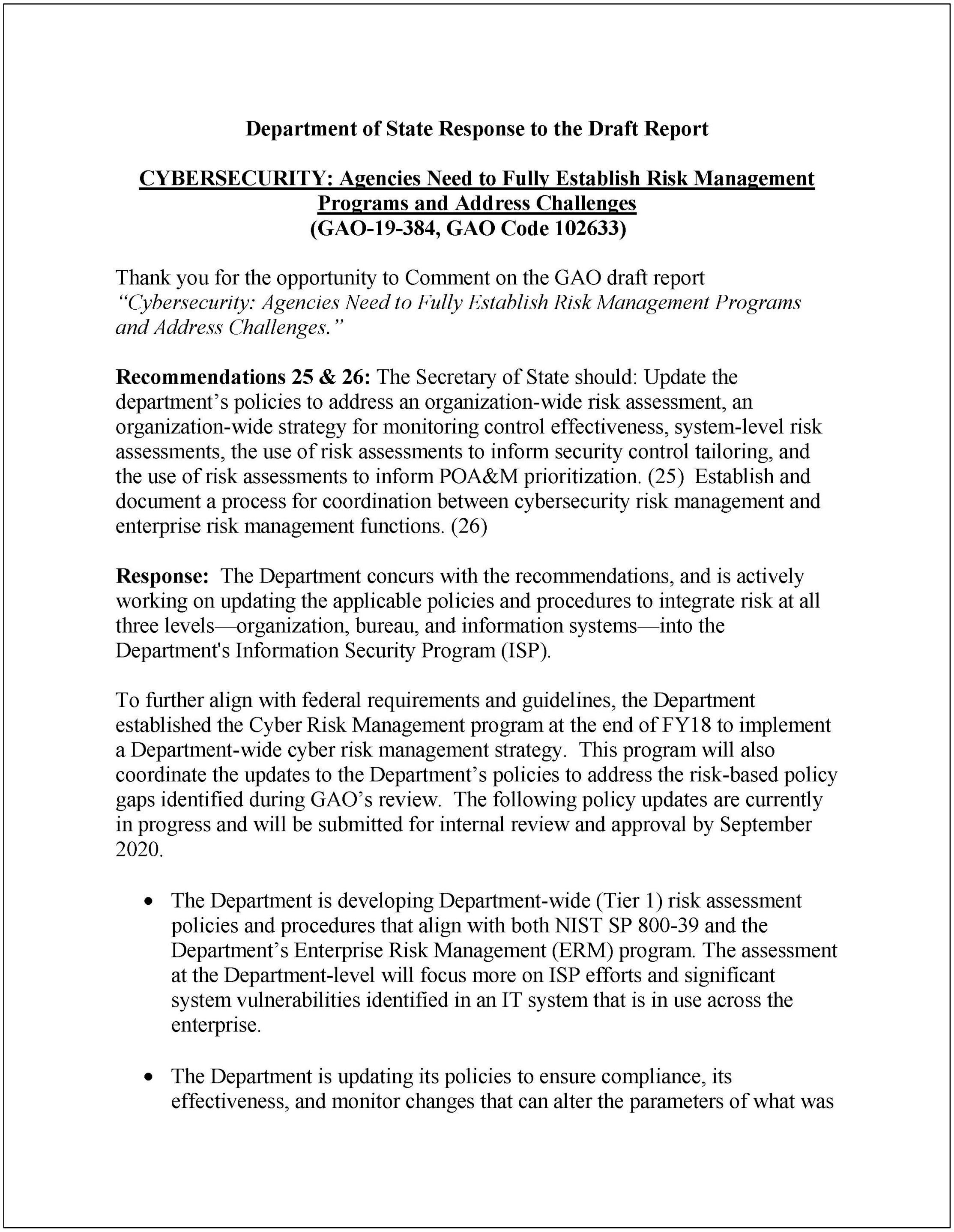
Sincerely,

Jeffrey C. Mo

Jeffrey C. Mounts (Acting)

Enclosure:
As stated

cc: GAO – Nick Marinos
IRM – Stuart McGuigan
OIG - Norman Brown



Department of State Response to the Draft Report

CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
(GAO-19-384, GAO Code 102633)

Thank you for the opportunity to Comment on the GAO draft report *"Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges."*

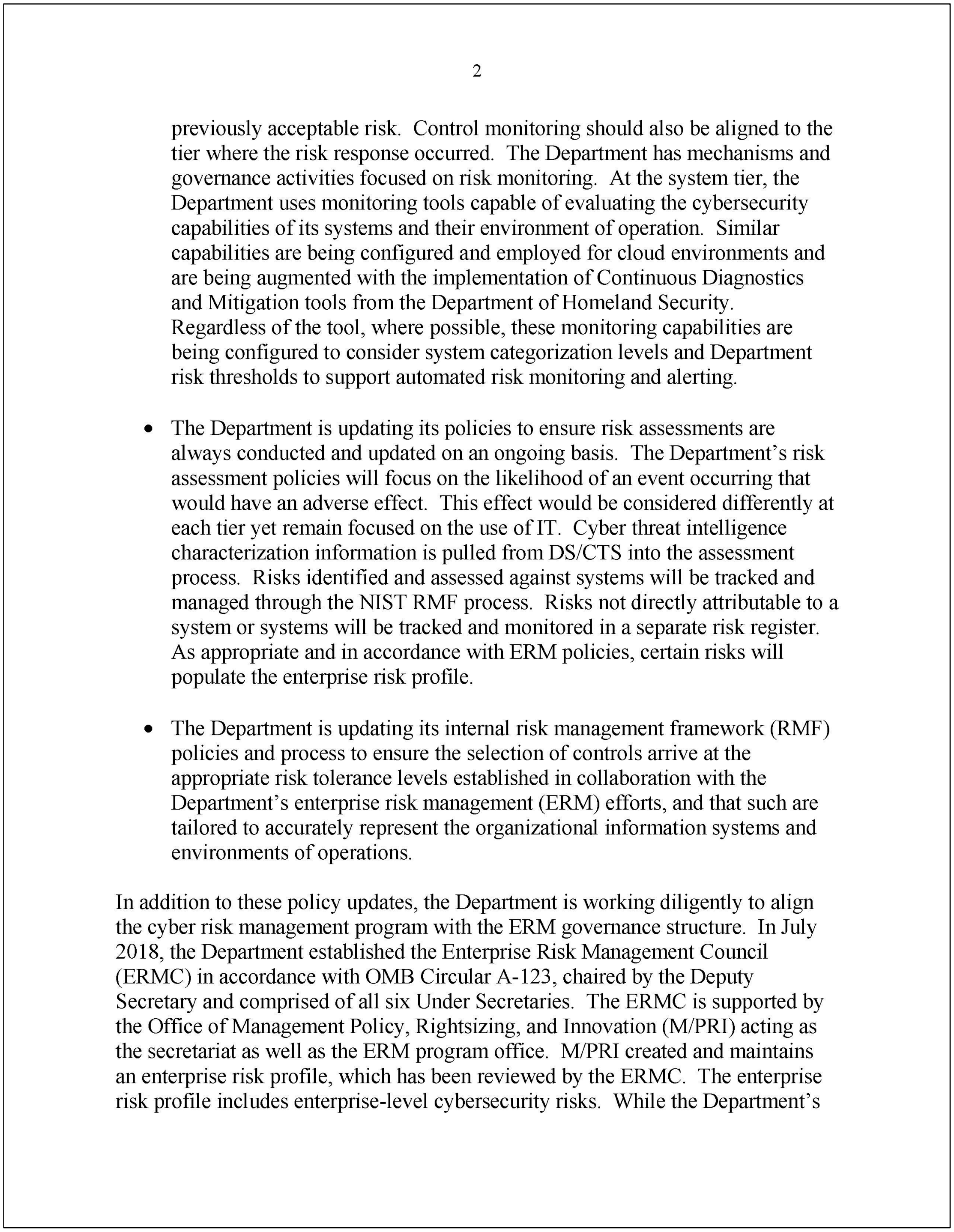
Recommendations 25 & 26: The Secretary of State should: Update the department's policies to address an organization-wide risk assessment, an organization-wide strategy for monitoring control effectiveness, system-level risk assessments, the use of risk assessments to inform security control tailoring, and the use of risk assessments to inform POA&M prioritization. (25) Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (26)

Response: The Department concurs with the recommendations, and is actively working on updating the applicable policies and procedures to integrate risk at all three levels—organization, bureau, and information systems—into the Department's Information Security Program (ISP).

To further align with federal requirements and guidelines, the Department established the Cyber Risk Management program at the end of FY18 to implement a Department-wide cyber risk management strategy. This program will also coordinate the updates to the Department's policies to address the risk-based policy gaps identified during GAO's review. The following policy updates are currently in progress and will be submitted for internal review and approval by September 2020.

- The Department is developing Department-wide (Tier 1) risk assessment policies and procedures that align with both NIST SP 800-39 and the Department's Enterprise Risk Management (ERM) program. The assessment at the Department-level will focus more on ISP efforts and significant system vulnerabilities identified in an IT system that is in use across the enterprise.

- The Department is updating its policies to ensure compliance, its effectiveness, and monitor changes that can alter the parameters of what was

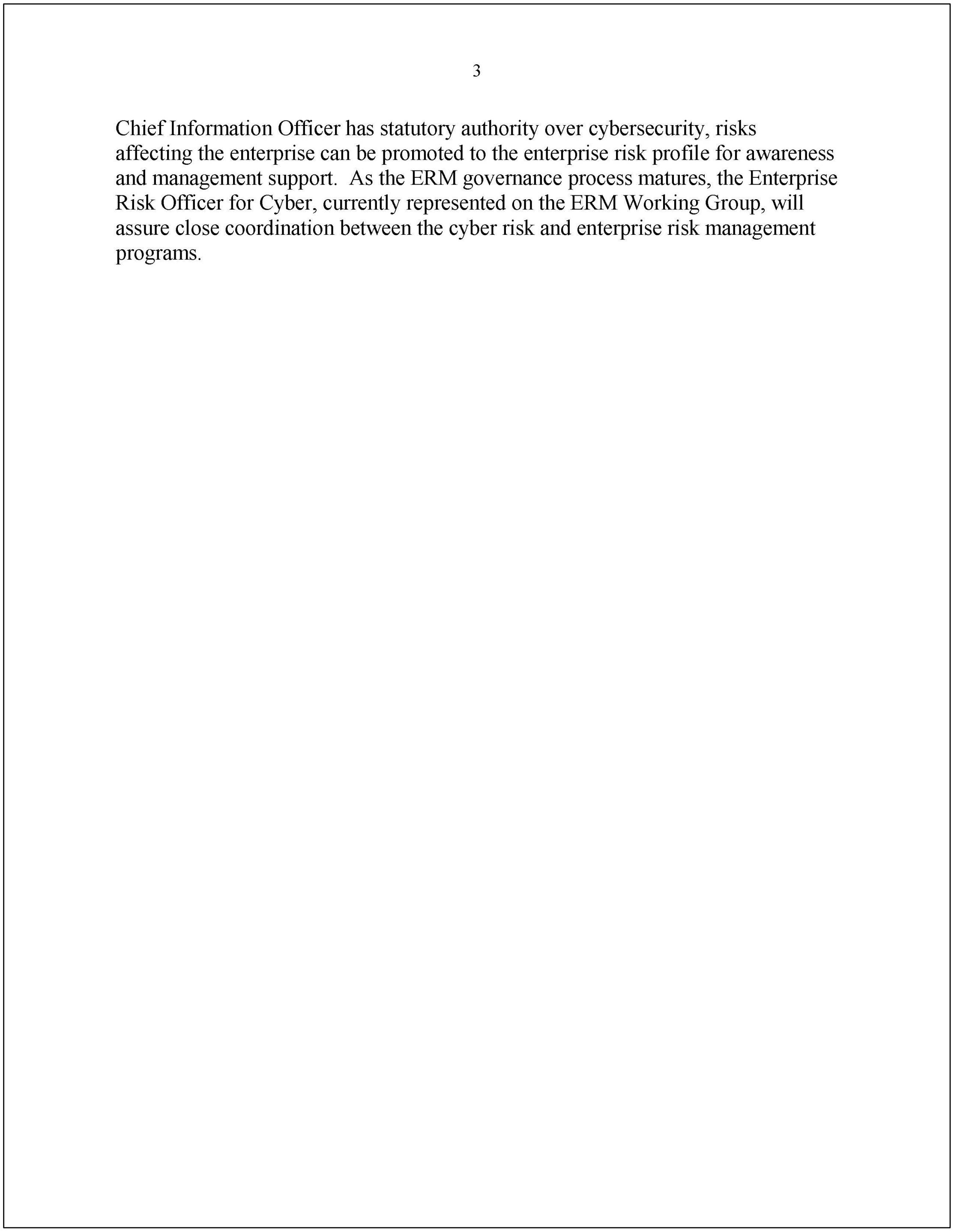


previously acceptable risk. Control monitoring should also be aligned to the tier where the risk response occurred. The Department has mechanisms and governance activities focused on risk monitoring. At the system tier, the Department uses monitoring tools capable of evaluating the cybersecurity capabilities of its systems and their environment of operation. Similar capabilities are being configured and employed for cloud environments and are being augmented with the implementation of Continuous Diagnostics and Mitigation tools from the Department of Homeland Security. Regardless of the tool, where possible, these monitoring capabilities are being configured to consider system categorization levels and Department risk thresholds to support automated risk monitoring and alerting.

- The Department is updating its policies to ensure risk assessments are always conducted and updated on an ongoing basis. The Department's risk assessment policies will focus on the likelihood of an event occurring that would have an adverse effect. This effect would be considered differently at each tier yet remain focused on the use of IT. Cyber threat intelligence characterization information is pulled from DS/CTS into the assessment process. Risks identified and assessed against systems will be tracked and managed through the NIST RMF process. Risks not directly attributable to a system or systems will be tracked and monitored in a separate risk register. As appropriate and in accordance with ERM policies, certain risks will populate the enterprise risk profile.

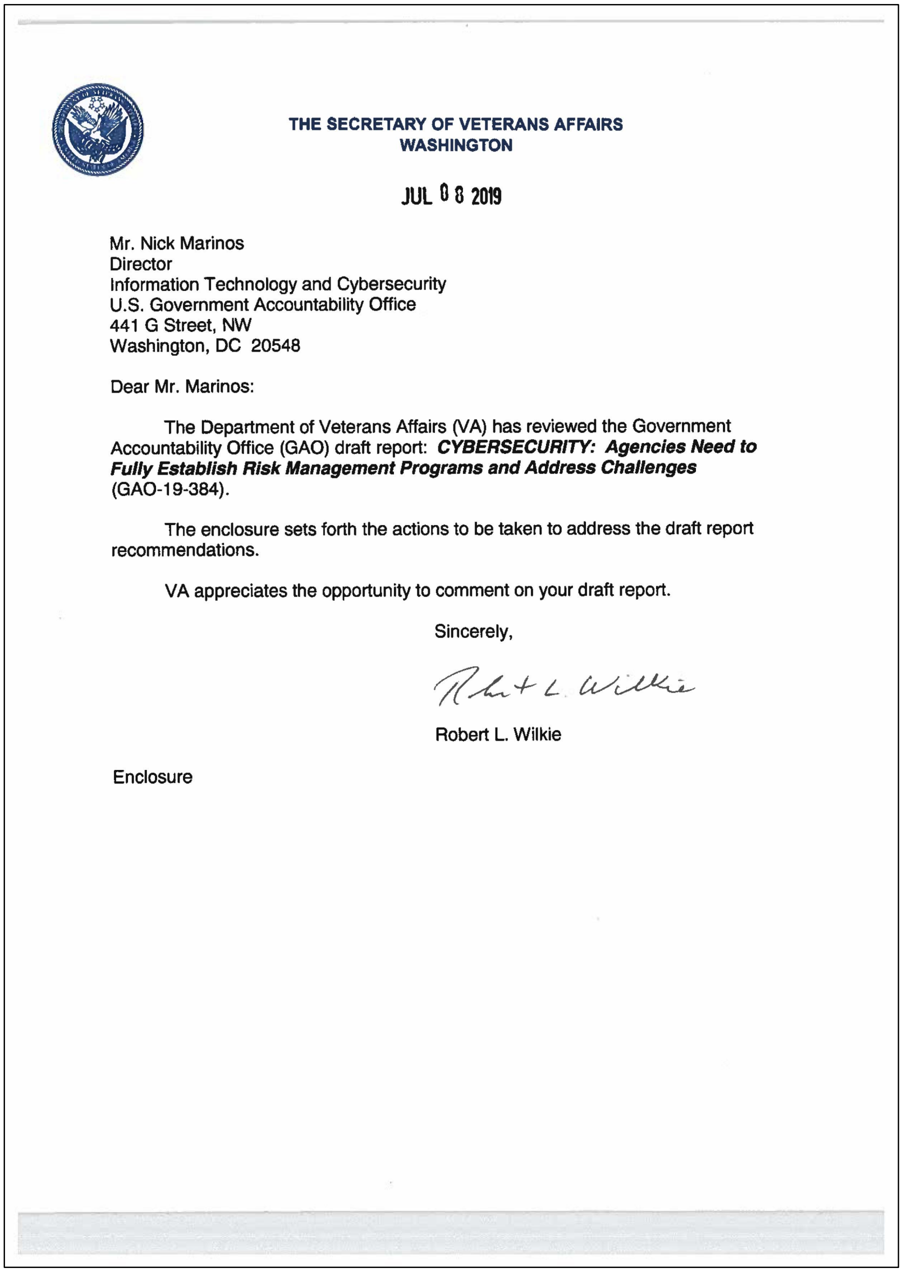
- The Department is updating its internal risk management framework (RMF) policies and process to ensure the selection of controls arrive at the appropriate risk tolerance levels established in collaboration with the Department's enterprise risk management (ERM) efforts, and that such are tailored to accurately represent the organizational information systems and environments of operations.

In addition to these policy updates, the Department is working diligently to align the cyber risk management program with the ERM governance structure. In July 2018, the Department established the Enterprise Risk Management Council (ERMC) in accordance with OMB Circular A-123, chaired by the Deputy Secretary and comprised of all six Under Secretaries. The ERMC is supported by the Office of Management Policy, Rightsizing, and Innovation (M/PRI) acting as the secretariat as well as the ERM program office. M/PRI created and maintains an enterprise risk profile, which has been reviewed by the ERMC. The enterprise risk profile includes enterprise-level cybersecurity risks. While the Department's



Chief Information Officer has statutory authority over cybersecurity, risks affecting the enterprise can be promoted to the enterprise risk profile for awareness and management support. As the ERM governance process matures, the Enterprise Risk Officer for Cyber, currently represented on the ERM Working Group, will assure close coordination between the cyber risk and enterprise risk management programs.

Appendix XVI: Comments from the Department of Veterans Affairs



THE SECRETARY OF VETERANS AFFAIRS
WASHINGTON

JUL 0 8 2019

Mr. Nick Marinos
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office (GAO) draft report: ***CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*** (GAO-19-384).

The enclosure sets forth the actions to be taken to address the draft report recommendations.

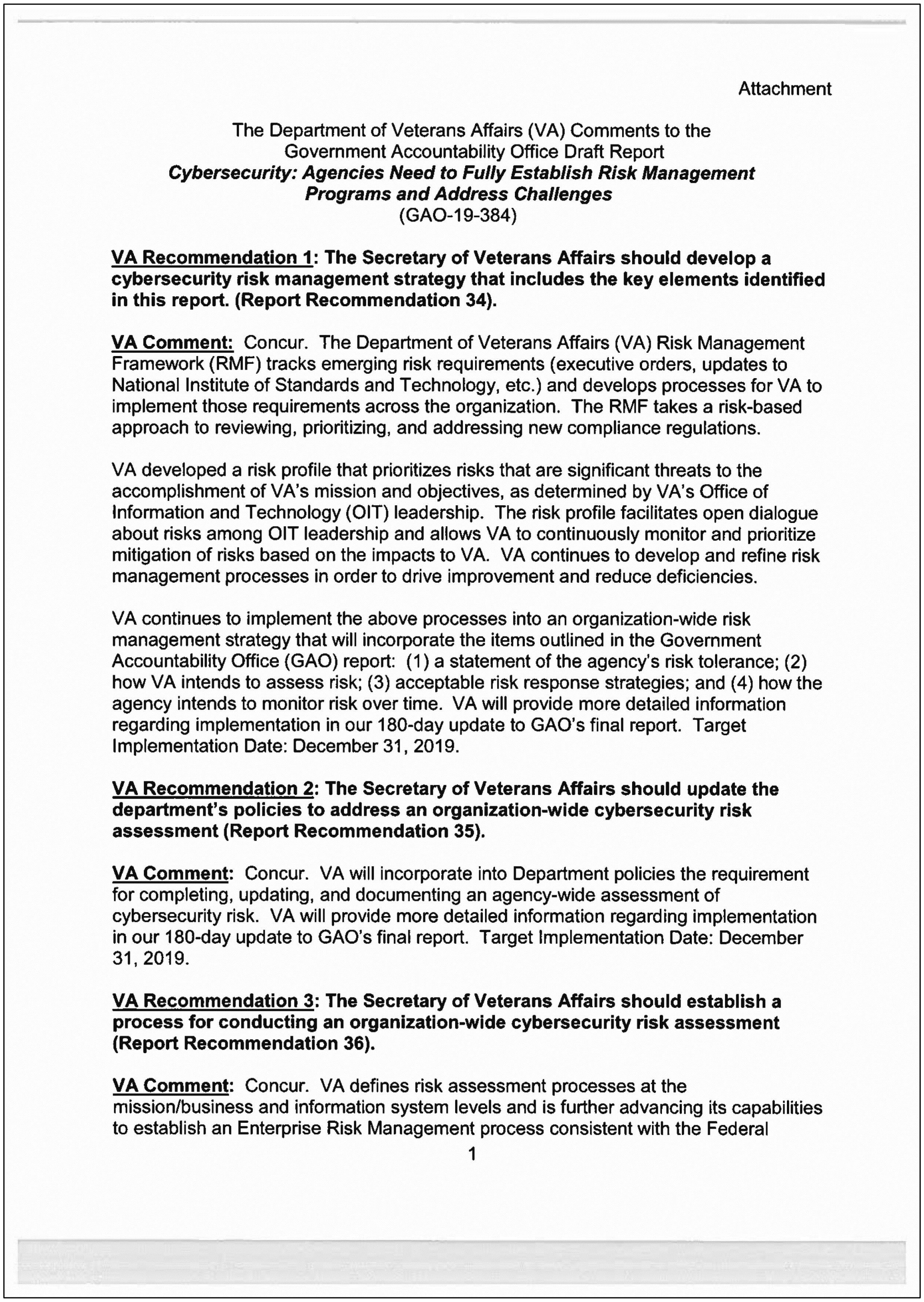
VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie

Enclosure

Appendix XVI: Comments from the Department of Veterans Affairs



Attachment

The Department of Veterans Affairs (VA) Comments to the
Government Accountability Office Draft Report
Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
(GAO-19-384)

VA Recommendation 1: The Secretary of Veterans Affairs should develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Report Recommendation 34).

VA Comment: Concur. The Department of Veterans Affairs (VA) Risk Management Framework (RMF) tracks emerging risk requirements (executive orders, updates to National Institute of Standards and Technology, etc.) and develops processes for VA to implement those requirements across the organization. The RMF takes a risk-based approach to reviewing, prioritizing, and addressing new compliance regulations.

VA developed a risk profile that prioritizes risks that are significant threats to the accomplishment of VA's mission and objectives, as determined by VA's Office of Information and Technology (OIT) leadership. The risk profile facilitates open dialogue about risks among OIT leadership and allows VA to continuously monitor and prioritize mitigation of risks based on the impacts to VA. VA continues to develop and refine risk management processes in order to drive improvement and reduce deficiencies.

VA continues to implement the above processes into an organization-wide risk management strategy that will incorporate the items outlined in the Government Accountability Office (GAO) report: (1) a statement of the agency's risk tolerance; (2) how VA intends to assess risk; (3) acceptable risk response strategies; and (4) how the agency intends to monitor risk over time. VA will provide more detailed information regarding implementation in our 180-day update to GAO's final report. Target Implementation Date: December 31, 2019.

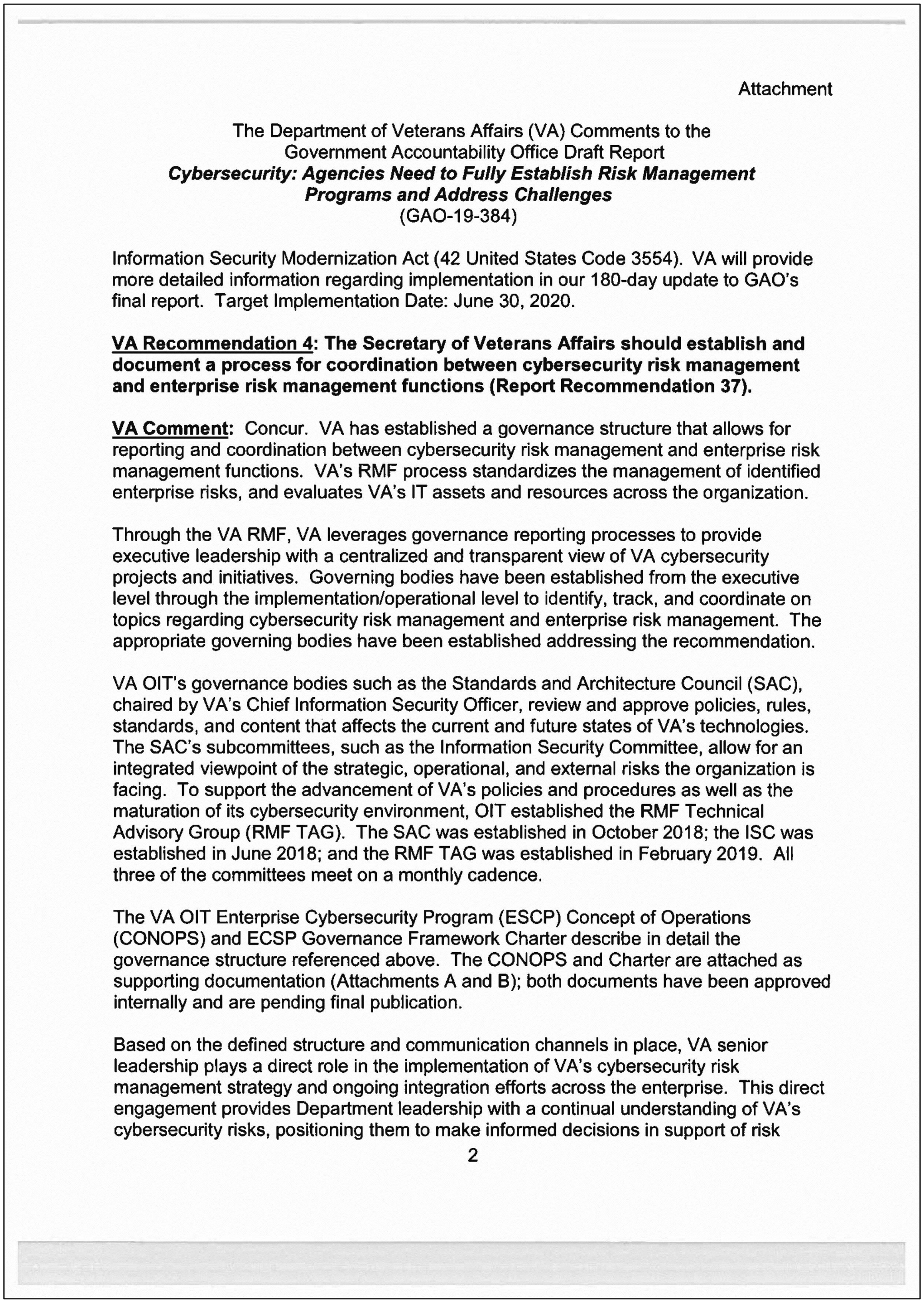
VA Recommendation 2: The Secretary of Veterans Affairs should update the department's policies to address an organization-wide cybersecurity risk assessment (Report Recommendation 35).

VA Comment: Concur. VA will incorporate into Department policies the requirement for completing, updating, and documenting an agency-wide assessment of cybersecurity risk. VA will provide more detailed information regarding implementation in our 180-day update to GAO's final report. Target Implementation Date: December 31, 2019.

VA Recommendation 3: The Secretary of Veterans Affairs should establish a process for conducting an organization-wide cybersecurity risk assessment (Report Recommendation 36).

VA Comment: Concur. VA defines risk assessment processes at the mission/business and information system levels and is further advancing its capabilities to establish an Enterprise Risk Management process consistent with the Federal

1



Attachment

The Department of Veterans Affairs (VA) Comments to the
Government Accountability Office Draft Report
Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
(GAO-19-384)

Information Security Modernization Act (42 United States Code 3554). VA will provide more detailed information regarding implementation in our 180-day update to GAO's final report. Target Implementation Date: June 30, 2020.

VA Recommendation 4: The Secretary of Veterans Affairs should establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions (Report Recommendation 37).

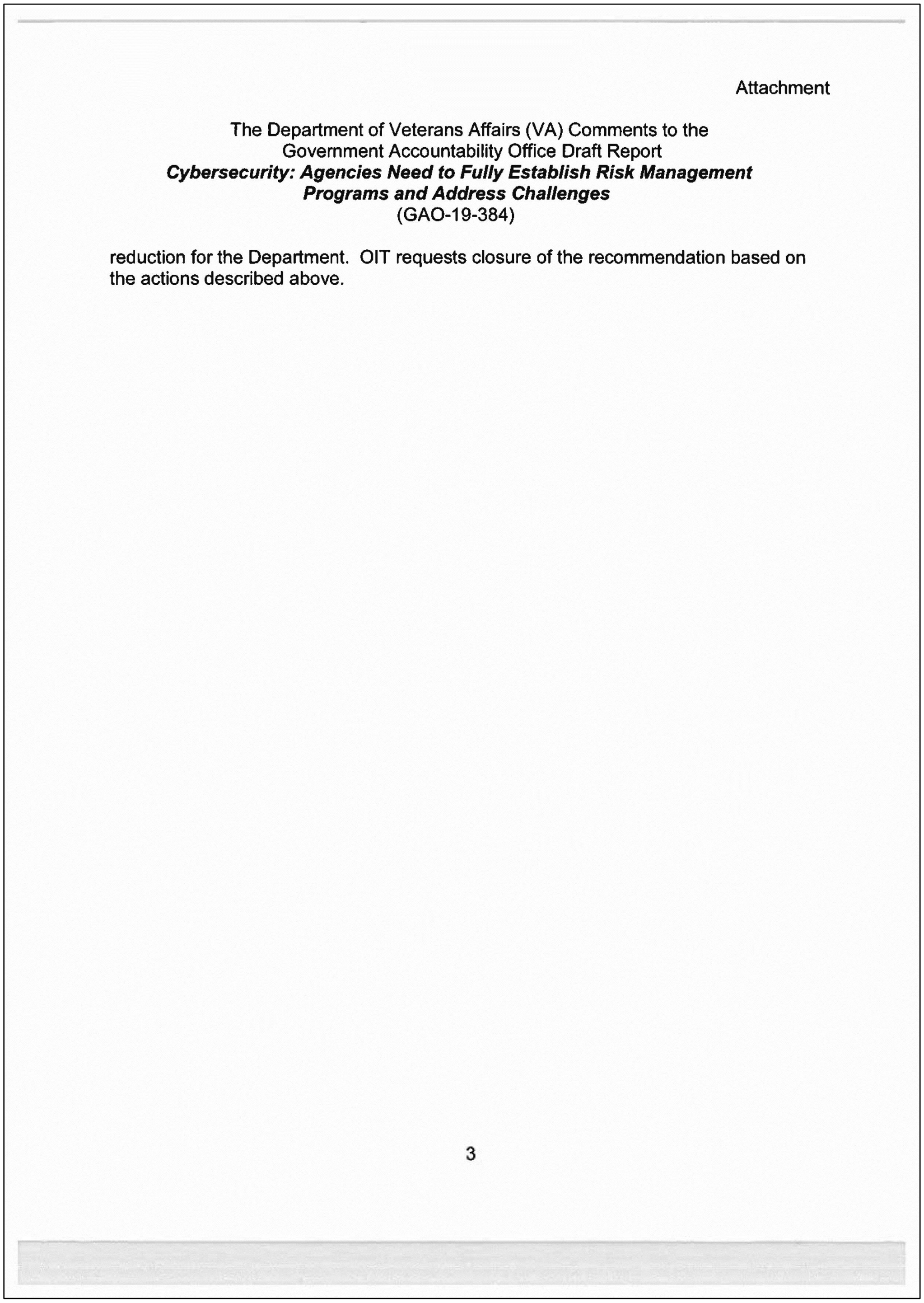
VA Comment: Concur. VA has established a governance structure that allows for reporting and coordination between cybersecurity risk management and enterprise risk management functions. VA's RMF process standardizes the management of identified enterprise risks, and evaluates VA's IT assets and resources across the organization.

Through the VA RMF, VA leverages governance reporting processes to provide executive leadership with a centralized and transparent view of VA cybersecurity projects and initiatives. Governing bodies have been established from the executive level through the implementation/operational level to identify, track, and coordinate on topics regarding cybersecurity risk management and enterprise risk management. The appropriate governing bodies have been established addressing the recommendation.

VA OIT's governance bodies such as the Standards and Architecture Council (SAC), chaired by VA's Chief Information Security Officer, review and approve policies, rules, standards, and content that affects the current and future states of VA's technologies. The SAC's subcommittees, such as the Information Security Committee, allow for an integrated viewpoint of the strategic, operational, and external risks the organization is facing. To support the advancement of VA's policies and procedures as well as the maturation of its cybersecurity environment, OIT established the RMF Technical Advisory Group (RMF TAG). The SAC was established in October 2018; the ISC was established in June 2018; and the RMF TAG was established in February 2019. All three of the committees meet on a monthly cadence.

The VA OIT Enterprise Cybersecurity Program (ESCP) Concept of Operations (CONOPS) and ECSP Governance Framework Charter describe in detail the governance structure referenced above. The CONOPS and Charter are attached as supporting documentation (Attachments A and B); both documents have been approved internally and are pending final publication.

Based on the defined structure and communication channels in place, VA senior leadership plays a direct role in the implementation of VA's cybersecurity risk management strategy and ongoing integration efforts across the enterprise. This direct engagement provides Department leadership with a continual understanding of VA's cybersecurity risks, positioning them to make informed decisions in support of risk



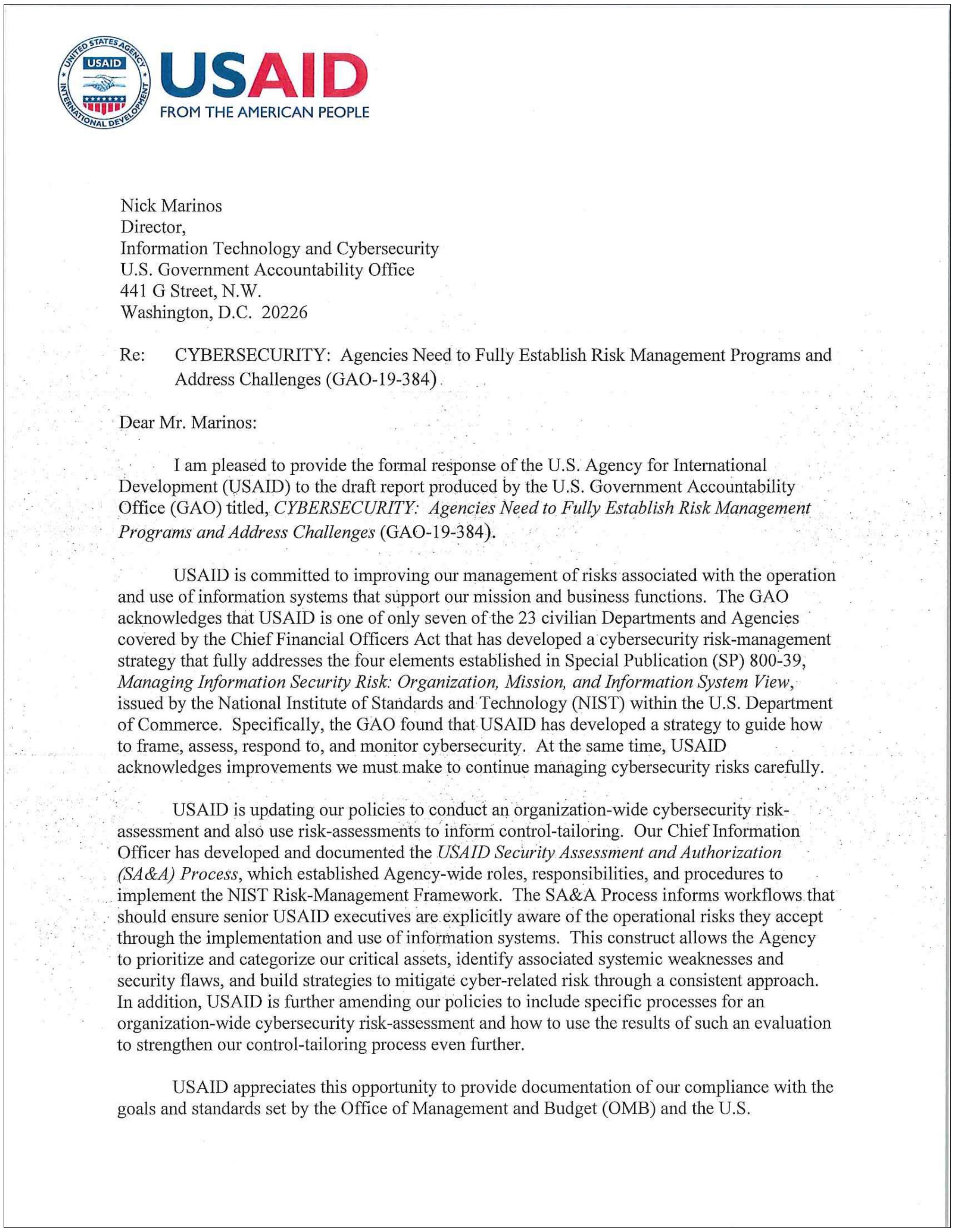
Attachment

The Department of Veterans Affairs (VA) Comments to the
Government Accountability Office Draft Report
Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
(GAO-19-384)

reduction for the Department. OIT requests closure of the recommendation based on the actions described above.

3

Appendix XVII: Comments from the U.S. Agency for International Development



USAID
FROM THE AMERICAN PEOPLE

Nick Marinos
Director,
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384)

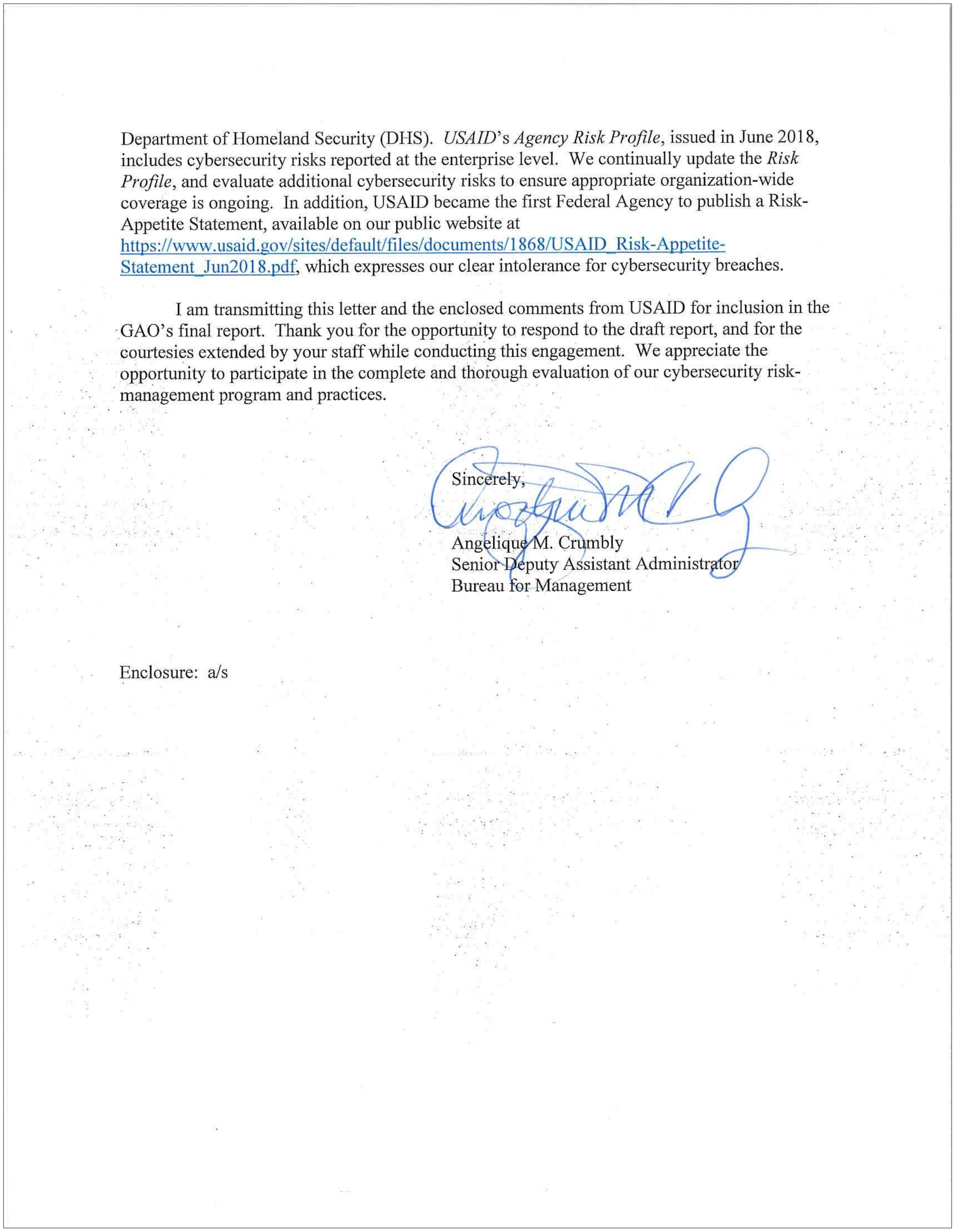
Dear Mr. Marinos:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, *CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges* (GAO-19-384).

USAID is committed to improving our management of risks associated with the operation and use of information systems that support our mission and business functions. The GAO acknowledges that USAID is one of only seven of the 23 civilian Departments and Agencies covered by the Chief Financial Officers Act that has developed a cybersecurity risk-management strategy that fully addresses the four elements established in Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, issued by the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce. Specifically, the GAO found that USAID has developed a strategy to guide how to frame, assess, respond to, and monitor cybersecurity. At the same time, USAID acknowledges improvements we must make to continue managing cybersecurity risks carefully.

USAID is updating our policies to conduct an organization-wide cybersecurity risk-assessment and also use risk-assessments to inform control-tailoring. Our Chief Information Officer has developed and documented the *USAID Security Assessment and Authorization (SA&A) Process*, which established Agency-wide roles, responsibilities, and procedures to implement the NIST Risk-Management Framework. The SA&A Process informs workflows that should ensure senior USAID executives are explicitly aware of the operational risks they accept through the implementation and use of information systems. This construct allows the Agency to prioritize and categorize our critical assets, identify associated systemic weaknesses and security flaws, and build strategies to mitigate cyber-related risk through a consistent approach. In addition, USAID is further amending our policies to include specific processes for an organization-wide cybersecurity risk-assessment and how to use the results of such an evaluation to strengthen our control-tailoring process even further.

USAID appreciates this opportunity to provide documentation of our compliance with the goals and standards set by the Office of Management and Budget (OMB) and the U.S.



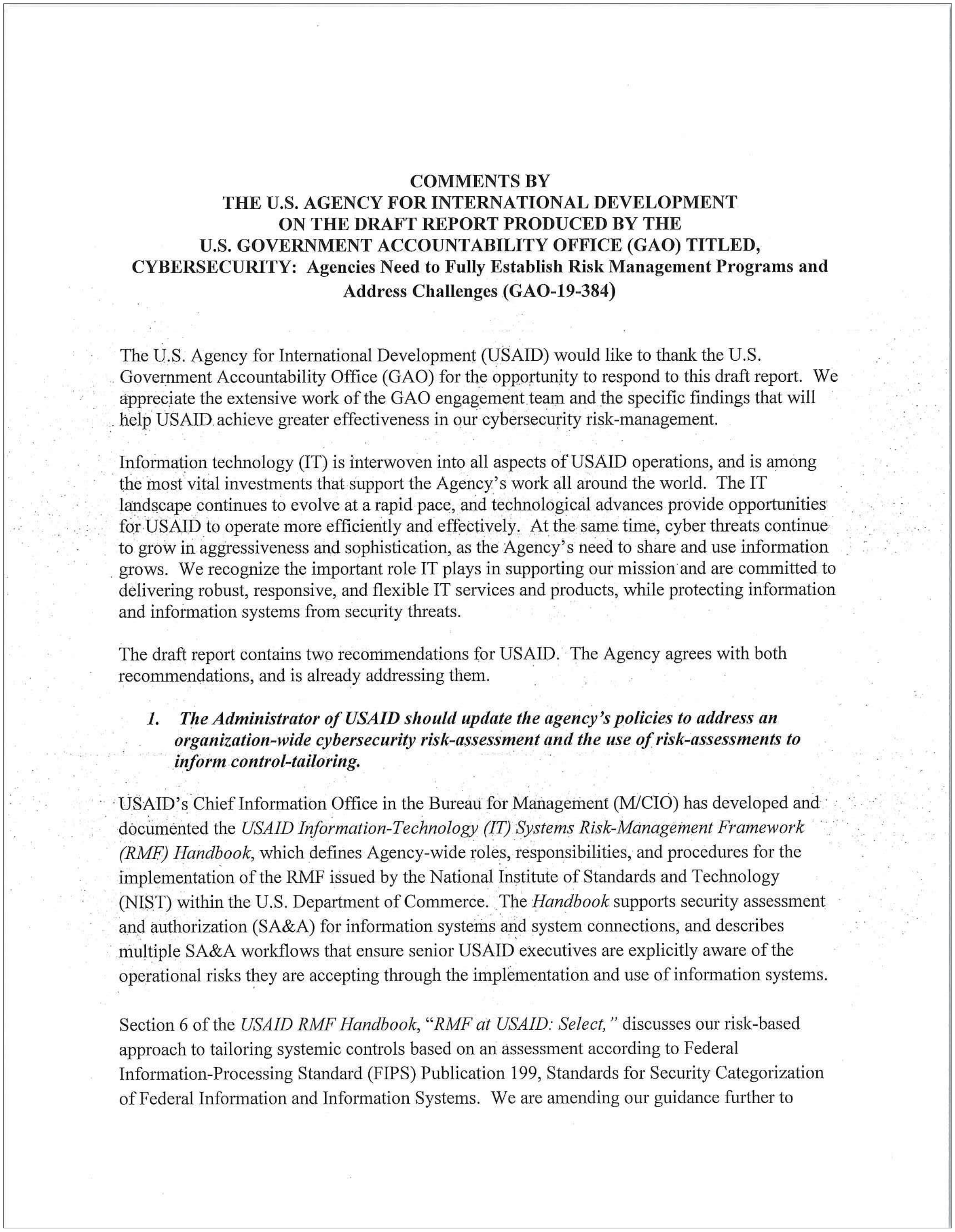
Department of Homeland Security (DHS). *USAID*'s *Agency Risk Profile*, issued in June 2018, includes cybersecurity risks reported at the enterprise level. We continually update the *Risk Profile*, and evaluate additional cybersecurity risks to ensure appropriate organization-wide coverage is ongoing. In addition, USAID became the first Federal Agency to publish a Risk-Appetite Statement, available on our public website at https://www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-Statement_Jun2018.pdf, which expresses our clear intolerance for cybersecurity breaches.

I am transmitting this letter and the enclosed comments from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our cybersecurity risk-management program and practices.

Sincerely,

Angelique M. Crumbly
Senior Deputy Assistant Administrator
Bureau for Management

Enclosure: a/s



**COMMENTS BY
THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT
ON THE DRAFT REPORT PRODUCED BY THE
U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) TITLED,
CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and
Address Challenges (GAO-19-384)**

The U.S. Agency for International Development (USAID) would like to thank the U.S. Government Accountability Office (GAO) for the opportunity to respond to this draft report. We appreciate the extensive work of the GAO engagement team and the specific findings that will help USAID achieve greater effectiveness in our cybersecurity risk-management.

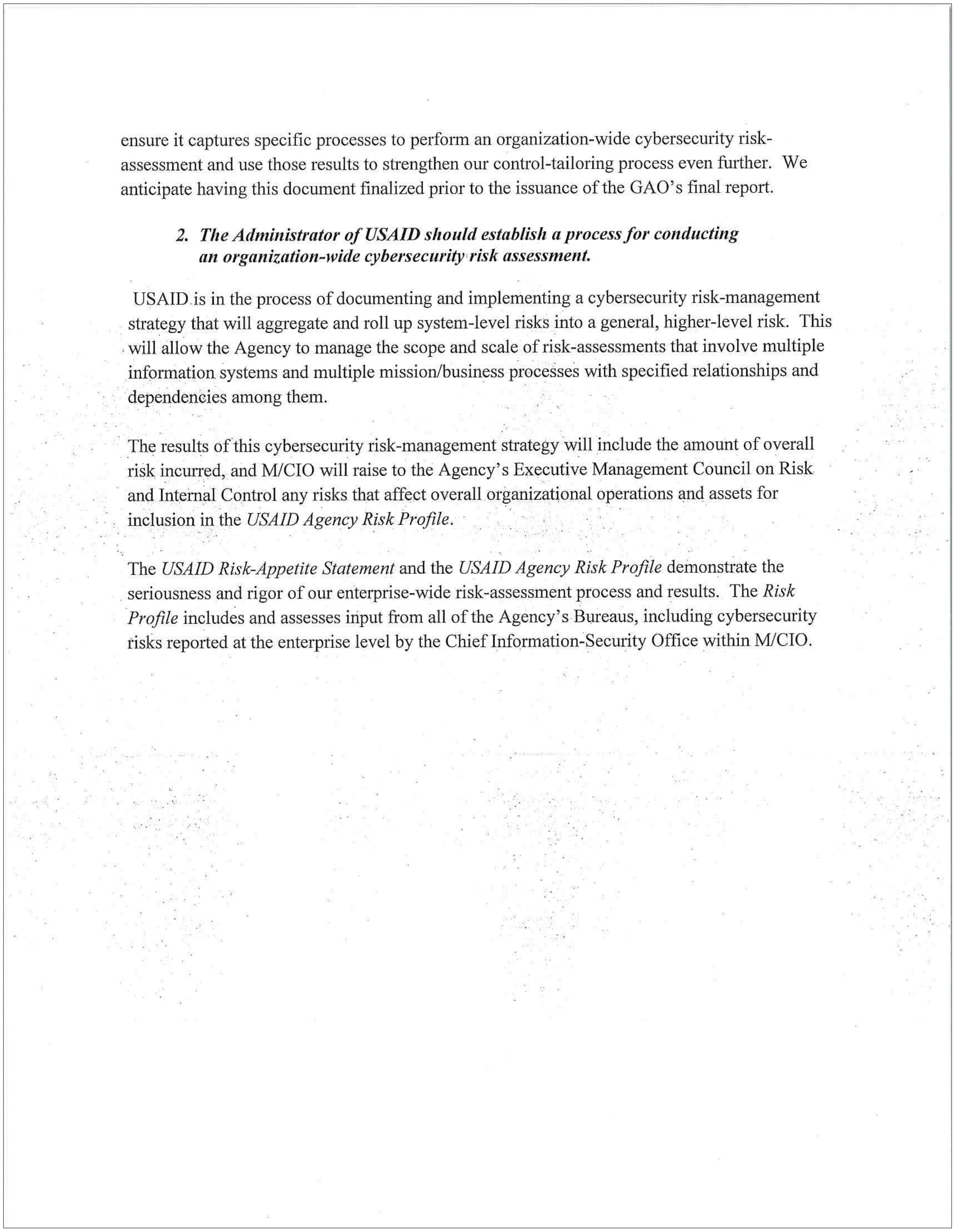
Information technology (IT) is interwoven into all aspects of USAID operations, and is among the most vital investments that support the Agency's work all around the world. The IT landscape continues to evolve at a rapid pace, and technological advances provide opportunities for USAID to operate more efficiently and effectively. At the same time, cyber threats continue to grow in aggressiveness and sophistication, as the Agency's need to share and use information grows. We recognize the important role IT plays in supporting our mission and are committed to delivering robust, responsive, and flexible IT services and products, while protecting information and information systems from security threats.

The draft report contains two recommendations for USAID. The Agency agrees with both recommendations, and is already addressing them.

1. ***The Administrator of USAID should update the agency's policies to address an organization-wide cybersecurity risk-assessment and the use of risk-assessments to inform control-tailoring.***

USAID's Chief Information Office in the Bureau for Management (M/CIO) has developed and documented the *USAID Information-Technology (IT) Systems Risk-Management Framework (RMF) Handbook*, which defines Agency-wide roles, responsibilities, and procedures for the implementation of the RMF issued by the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce. The *Handbook* supports security assessment and authorization (SA&A) for information systems and system connections, and describes multiple SA&A workflows that ensure senior USAID executives are explicitly aware of the operational risks they are accepting through the implementation and use of information systems.

Section 6 of the *USAID RMF Handbook*, "*RMF at USAID: Select,*" discusses our risk-based approach to tailoring systemic controls based on an assessment according to Federal Information-Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems. We are amending our guidance further to



ensure it captures specific processes to perform an organization-wide cybersecurity risk-assessment and use those results to strengthen our control-tailoring process even further. We anticipate having this document finalized prior to the issuance of the GAO's final report.

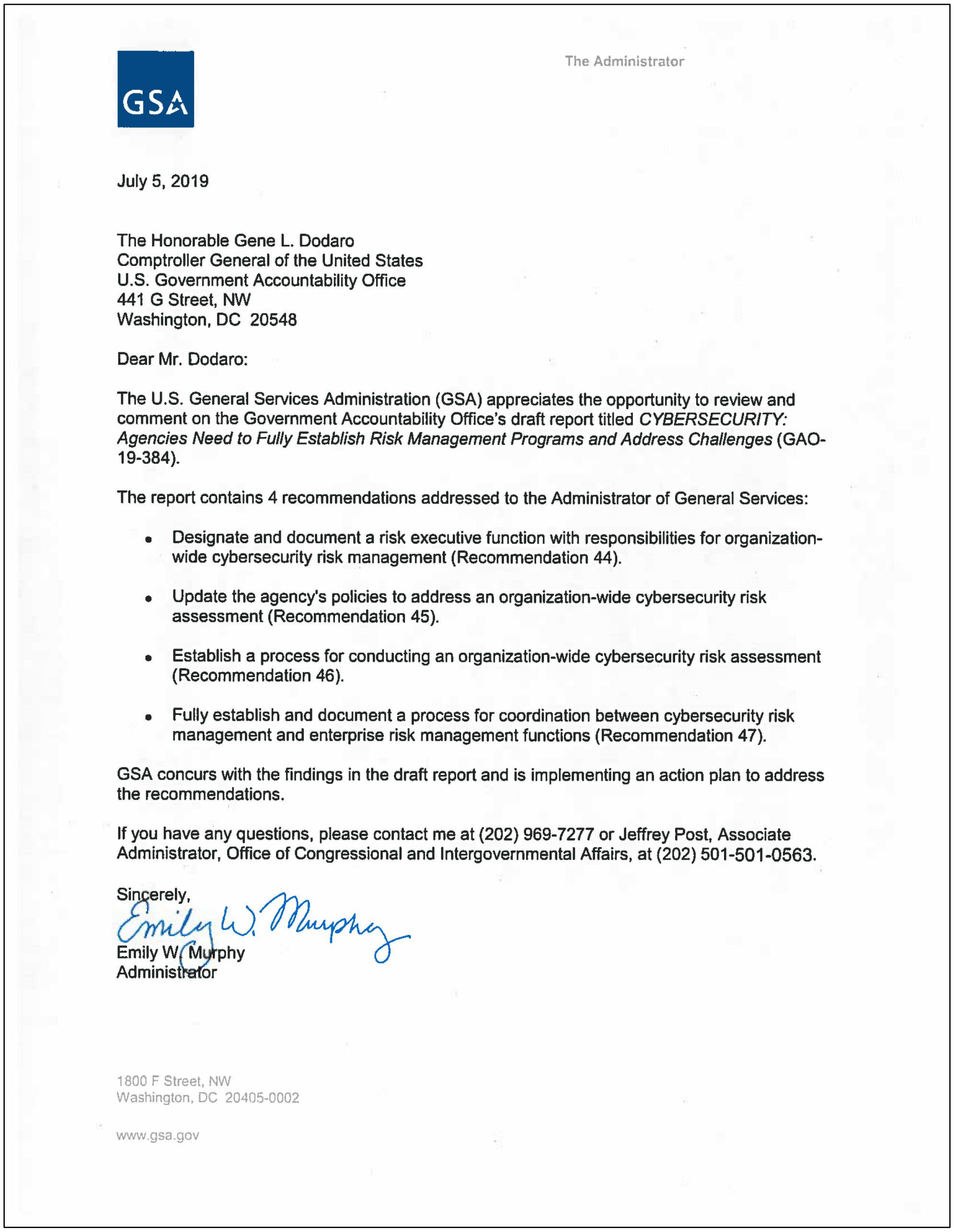
2. ***The Administrator of USAID should establish a process for conducting an organization-wide cybersecurity risk assessment.***

USAID is in the process of documenting and implementing a cybersecurity risk-management strategy that will aggregate and roll up system-level risks into a general, higher-level risk. This will allow the Agency to manage the scope and scale of risk-assessments that involve multiple information systems and multiple mission/business processes with specified relationships and dependencies among them.

The results of this cybersecurity risk-management strategy will include the amount of overall risk incurred, and M/CIO will raise to the Agency's Executive Management Council on Risk and Internal Control any risks that affect overall organizational operations and assets for inclusion in the *USAID Agency Risk Profile*.

The *USAID Risk-Appetite Statement* and the *USAID Agency Risk Profile* demonstrate the seriousness and rigor of our enterprise-wide risk-assessment process and results. The *Risk Profile* includes and assesses input from all of the Agency's Bureaus, including cybersecurity risks reported at the enterprise level by the Chief Information-Security Office within M/CIO.

Appendix XVIII: Comments from the General Services Administration



GSA

The Administrator

July 5, 2019

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the Government Accountability Office's draft report titled *CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges* (GAO-19-384).

The report contains 4 recommendations addressed to the Administrator of General Services:

- Designate and document a risk executive function with responsibilities for organization-wide cybersecurity risk management (Recommendation 44).
- Update the agency's policies to address an organization-wide cybersecurity risk assessment (Recommendation 45).
- Establish a process for conducting an organization-wide cybersecurity risk assessment (Recommendation 46).
- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions (Recommendation 47).

GSA concurs with the findings in the draft report and is implementing an action plan to address the recommendations.

If you have any questions, please contact me at (202) 969-7277 or Jeffrey Post, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-501-0563.

Sincerely,

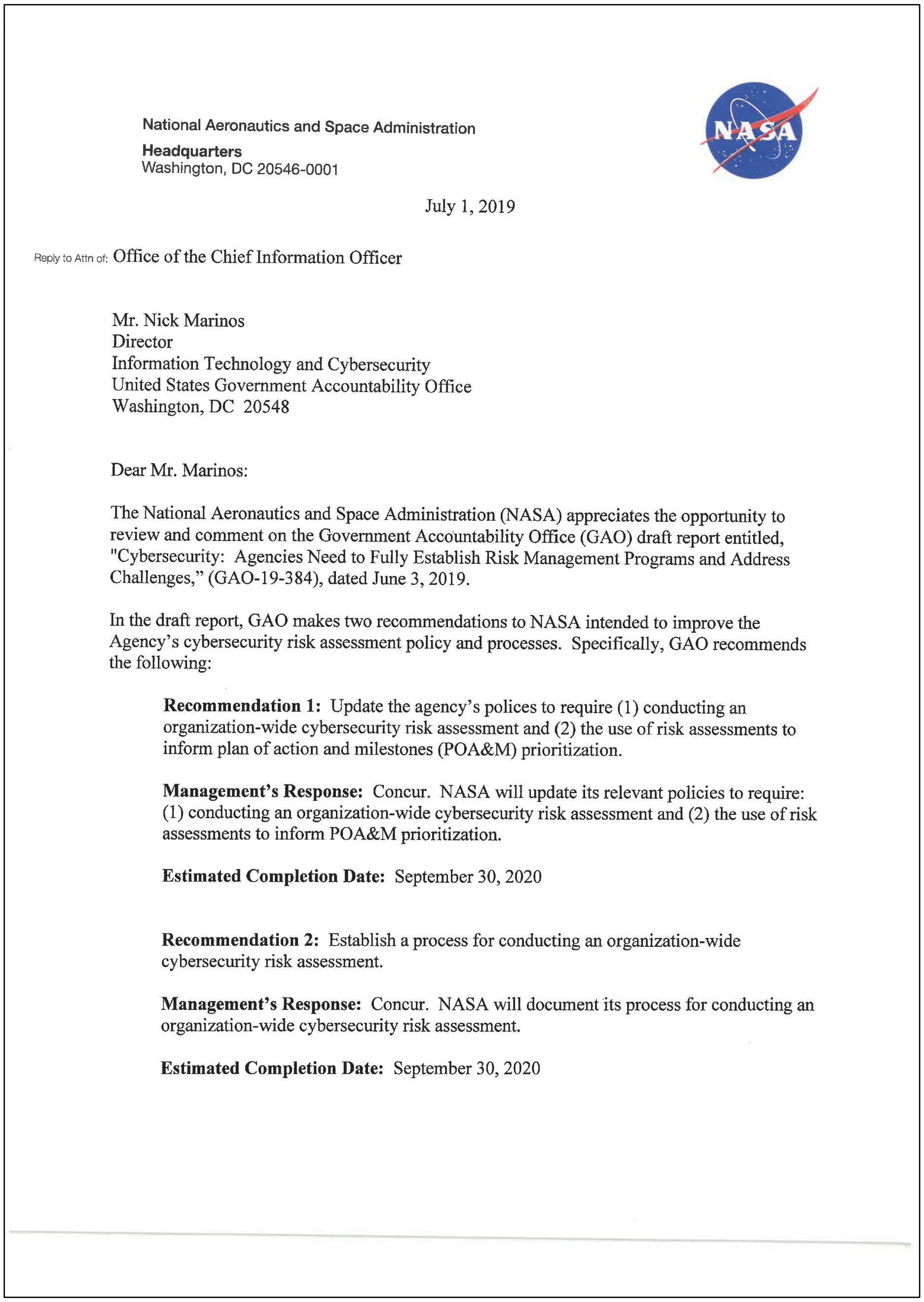
Emily W. Murphy

Emily W. Murphy
Administrator

1800 F Street, NW
Washington, DC 20405-0002

www.gsa.gov

Appendix XIX: Comments from the National Aeronautics and Space Administration



National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001

July 1, 2019

Reply to Attn of: Office of the Chief Information Officer

Mr. Nick Marinos
Director
Information Technology and Cybersecurity
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Marinos:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges," (GAO-19-384), dated June 3, 2019.

In the draft report, GAO makes two recommendations to NASA intended to improve the Agency's cybersecurity risk assessment policy and processes. Specifically, GAO recommends the following:

Recommendation 1: Update the agency's polices to require (1) conducting an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform plan of action and milestones (POA&M) prioritization.

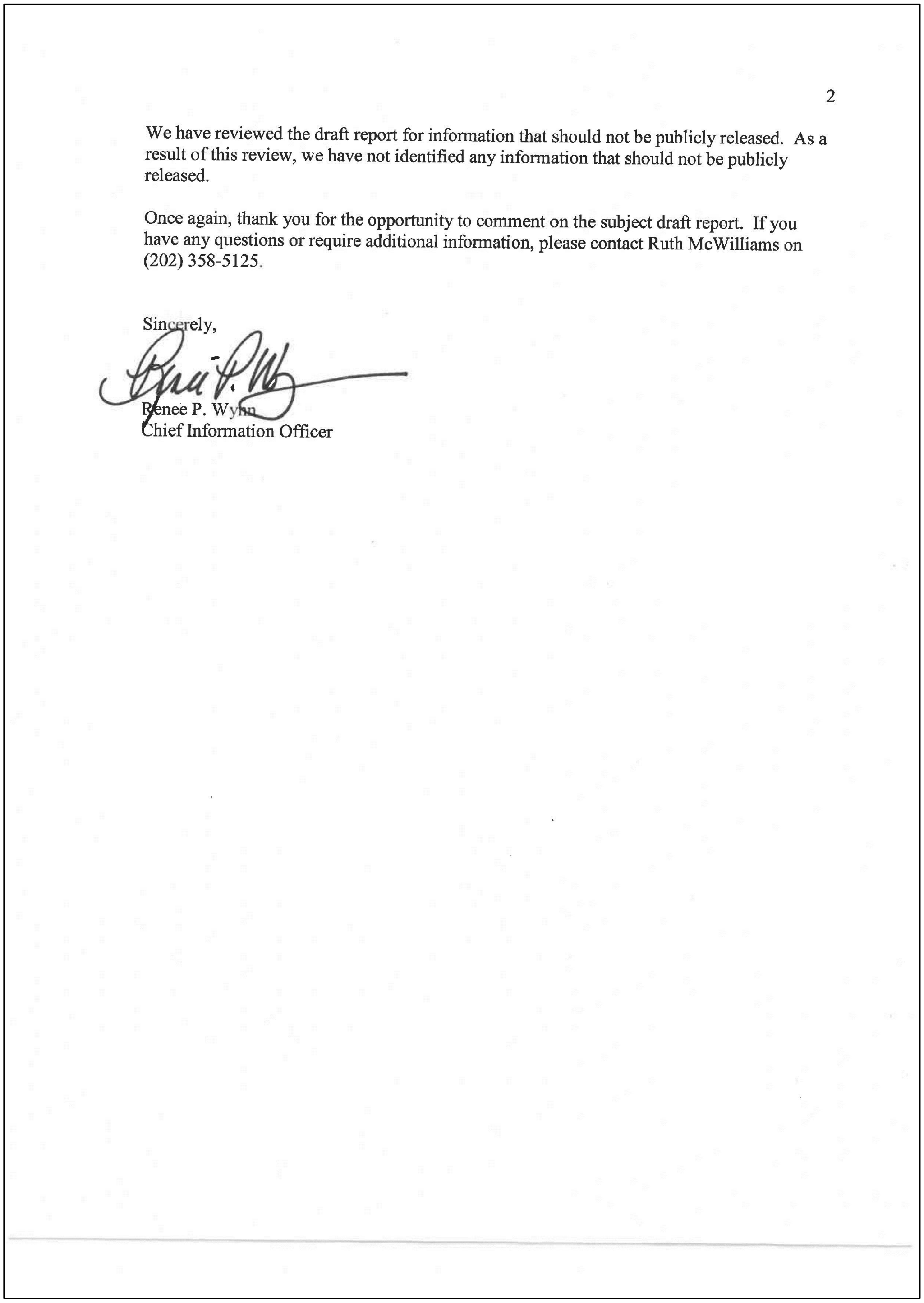
Management's Response: Concur. NASA will update its relevant policies to require: (1) conducting an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform POA&M prioritization.

Estimated Completion Date: September 30, 2020

Recommendation 2: Establish a process for conducting an organization-wide cybersecurity risk assessment.

Management's Response: Concur. NASA will document its process for conducting an organization-wide cybersecurity risk assessment.

Estimated Completion Date: September 30, 2020



2

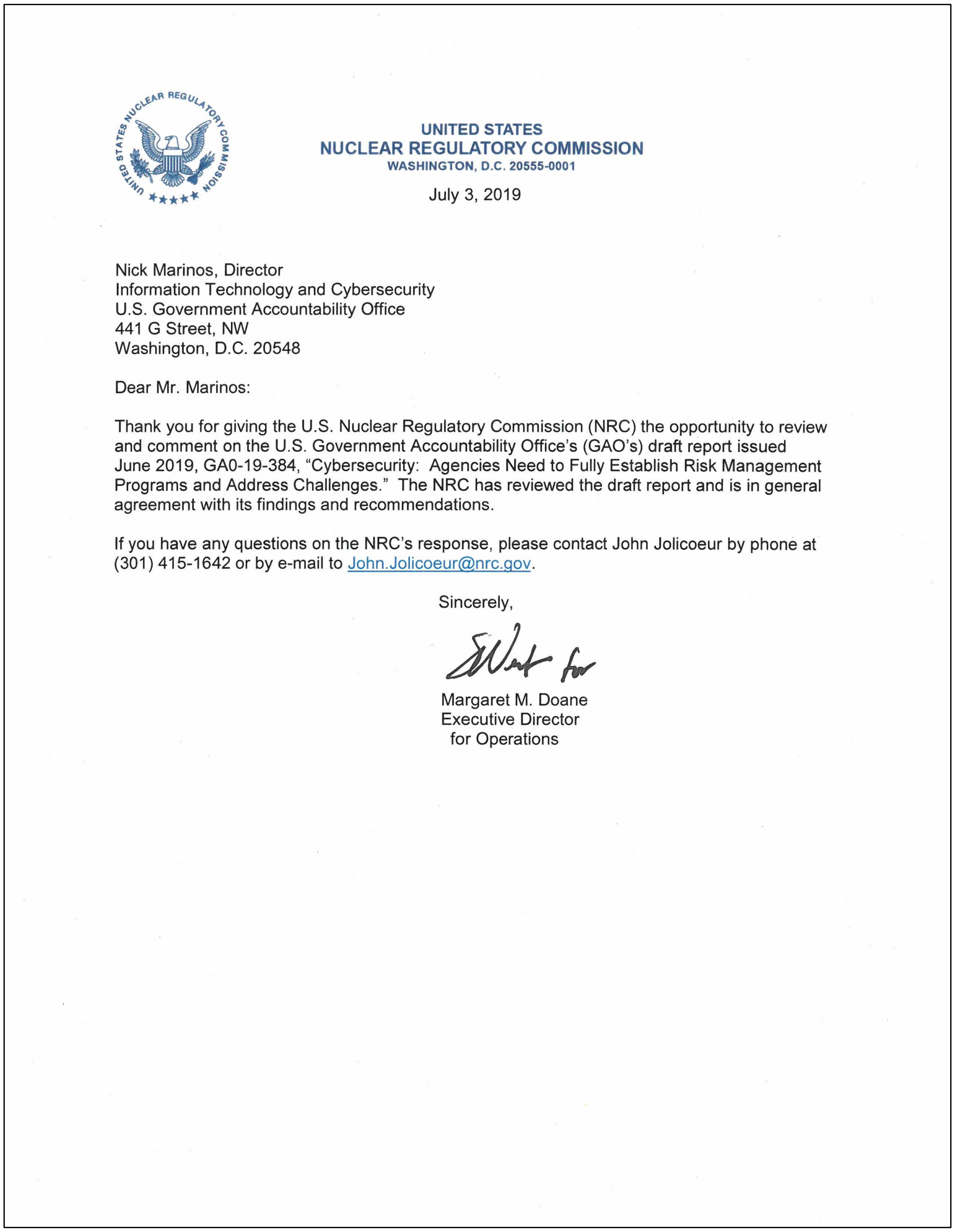
We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Ruth McWilliams on (202) 358-5125.

Sincerely,

Renee P. Wynn
Chief Information Officer

Appendix XX: Comments from the Nuclear Regulatory Commission



UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

July 3, 2019

Nick Marinos, Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for giving the U.S. Nuclear Regulatory Commission (NRC) the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report issued June 2019, GA0-19-384, "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges." The NRC has reviewed the draft report and is in general agreement with its findings and recommendations.

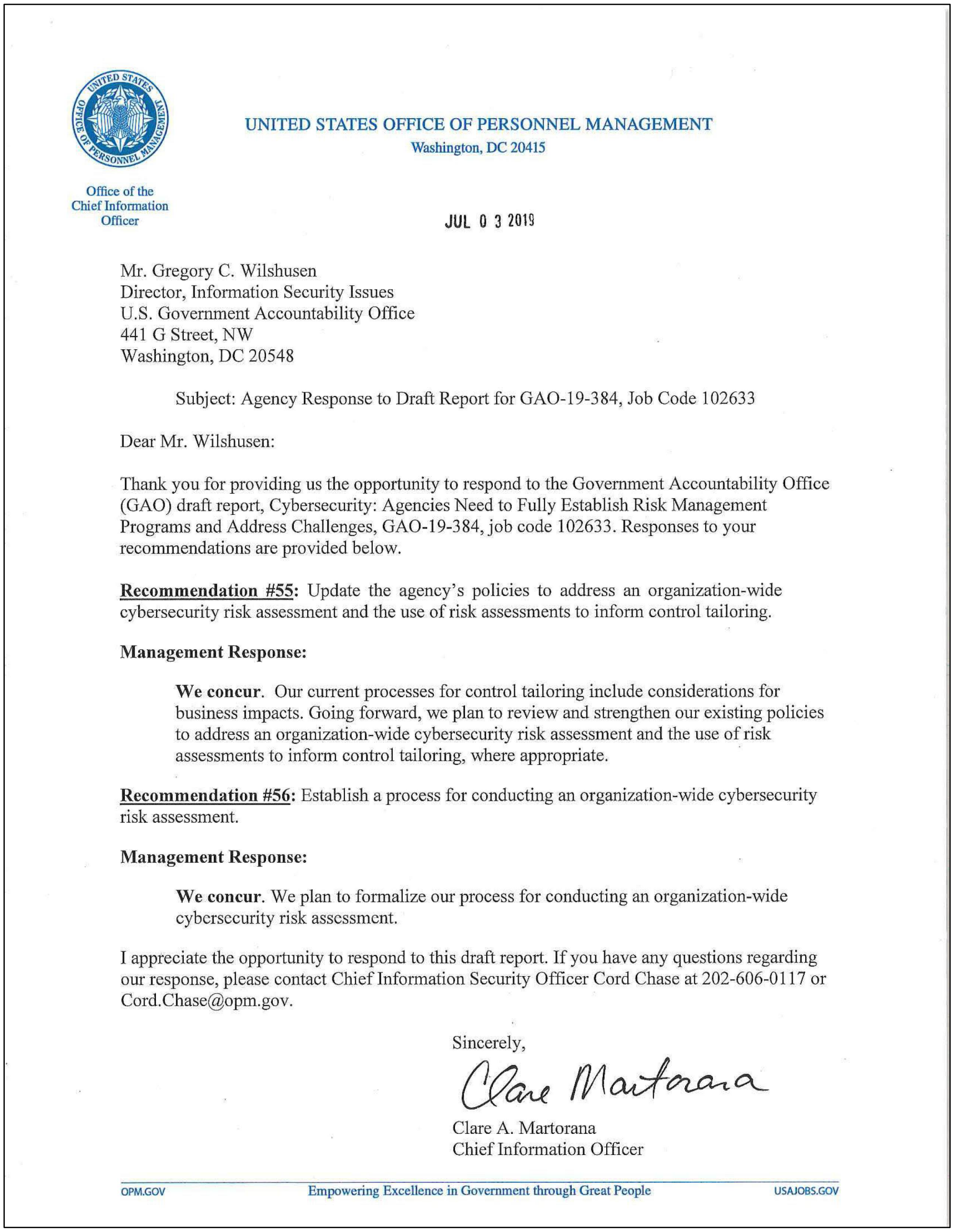
If you have any questions on the NRC's response, please contact John Jolicoeur by phone at (301) 415-1642 or by e-mail to John.Jolicoeur@nrc.gov.

Sincerely,

SWest for

Margaret M. Doane
Executive Director
for Operations

Appendix XXI: Comments from the Office of Personnel Management



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Chief Information
Officer

JUL 0 3 2019

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Subject: Agency Response to Draft Report for GAO-19-384, Job Code 102633

Dear Mr. Wilshusen:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges, GAO-19-384, job code 102633. Responses to your recommendations are provided below.

Recommendation #55: Update the agency's policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform control tailoring.

Management Response:

We concur. Our current processes for control tailoring include considerations for business impacts. Going forward, we plan to review and strengthen our existing policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform control tailoring, where appropriate.

Recommendation #56: Establish a process for conducting an organization-wide cybersecurity risk assessment.

Management Response:

We concur. We plan to formalize our process for conducting an organization-wide cybersecurity risk assessment.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Chief Information Security Officer Cord Chase at 202-606-0117 or Cord.Chase@opm.gov.

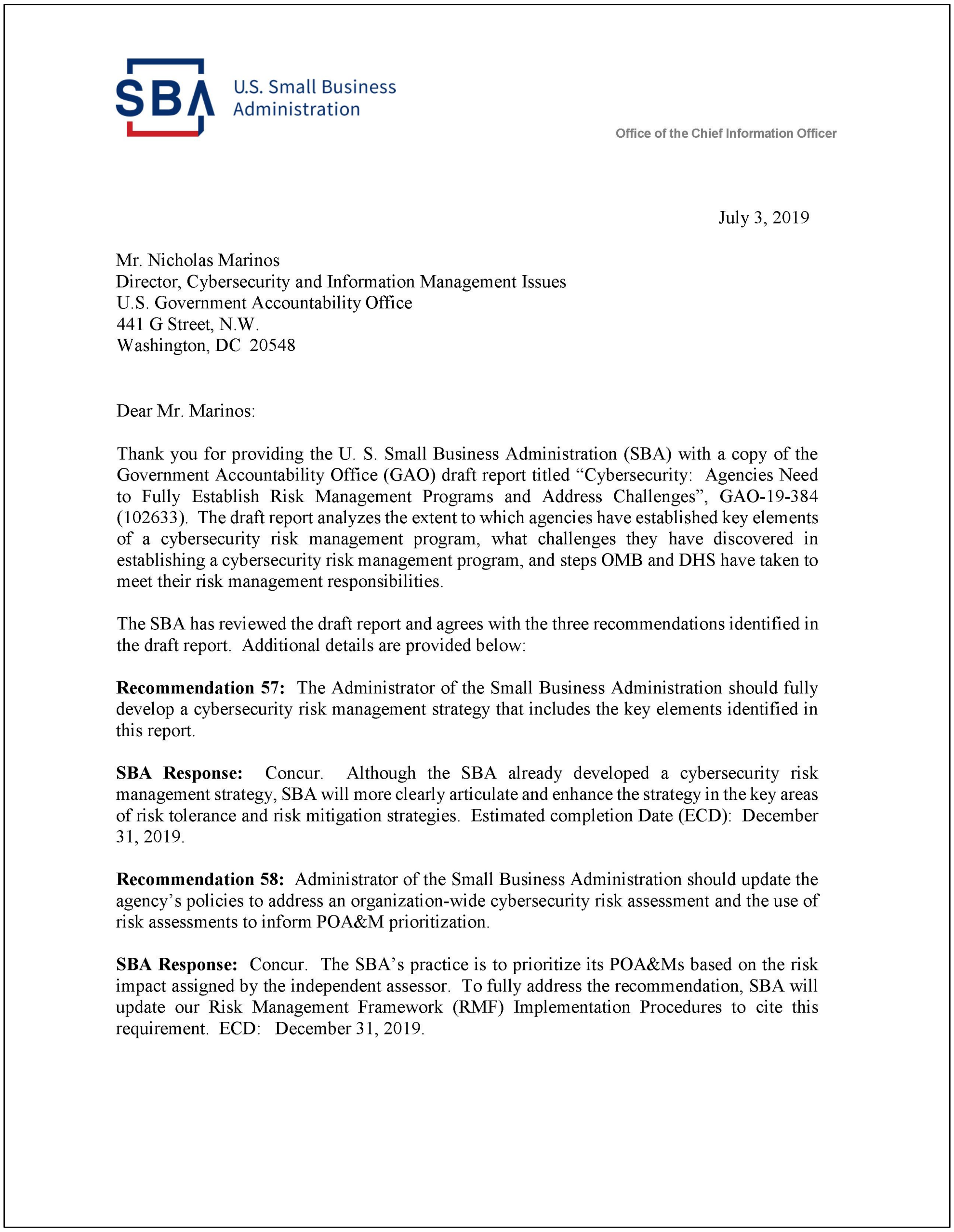
Sincerely,

Clare Martorana

Clare A. Martorana
Chief Information Officer

OPM.GOV Empowering Excellence in Government through Great People USAJOBS.GOV

Appendix XXII: Comments from the Small Business Administration



SBA U.S. Small Business Administration

Office of the Chief Information Officer

July 3, 2019

Mr. Nicholas Marinos
Director, Cybersecurity and Information Management Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Marinos:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges", GAO-19-384 (102633). The draft report analyzes the extent to which agencies have established key elements of a cybersecurity risk management program, what challenges they have discovered in establishing a cybersecurity risk management program, and steps OMB and DHS have taken to meet their risk management responsibilities.

The SBA has reviewed the draft report and agrees with the three recommendations identified in the draft report. Additional details are provided below:

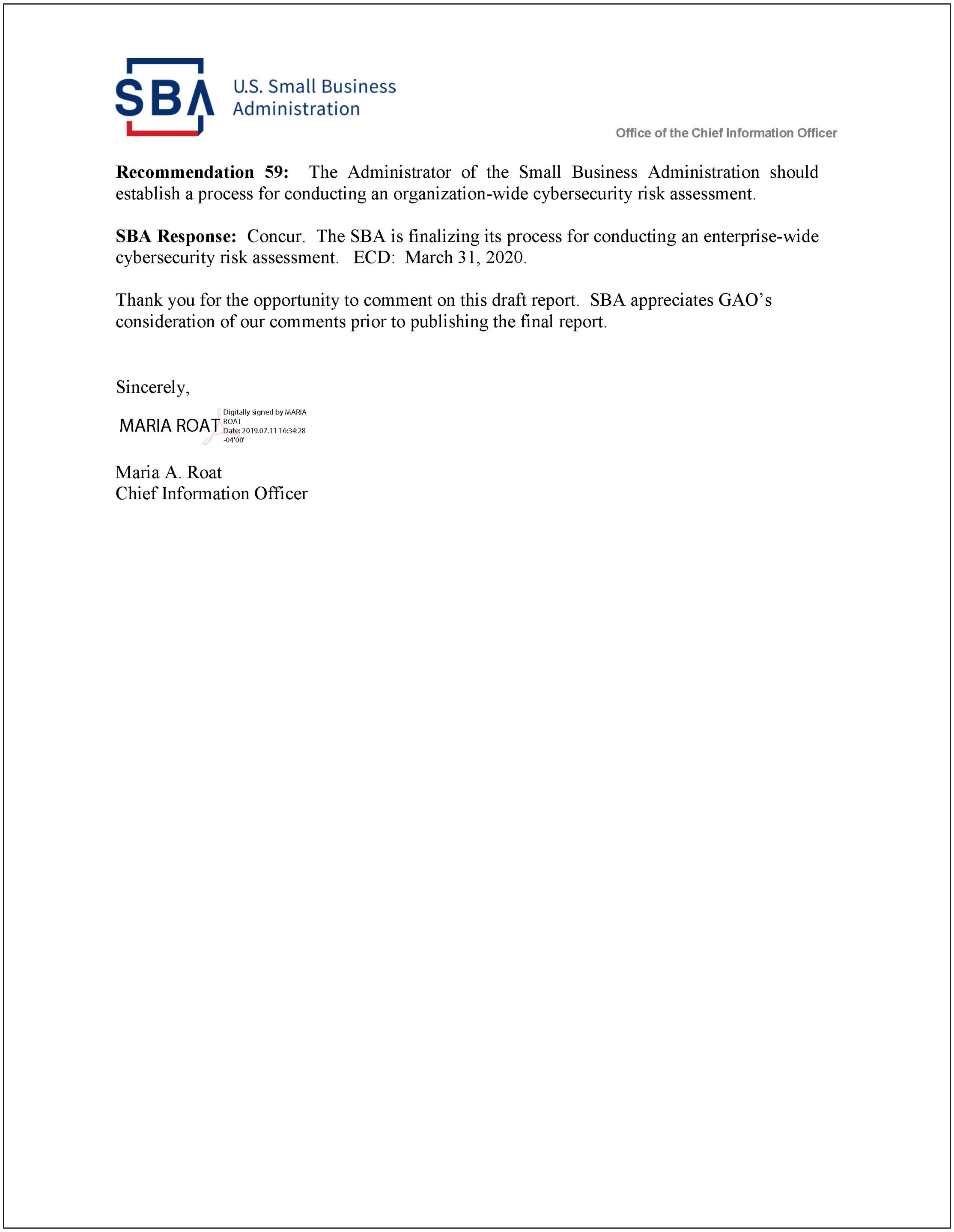
Recommendation 57: The Administrator of the Small Business Administration should fully develop a cybersecurity risk management strategy that includes the key elements identified in this report.

SBA Response: Concur. Although the SBA already developed a cybersecurity risk management strategy, SBA will more clearly articulate and enhance the strategy in the key areas of risk tolerance and risk mitigation strategies. Estimated completion Date (ECD): December 31, 2019.

Recommendation 58: Administrator of the Small Business Administration should update the agency's policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform POA&M prioritization.

SBA Response: Concur. The SBA's practice is to prioritize its POA&Ms based on the risk impact assigned by the independent assessor. To fully address the recommendation, SBA will update our Risk Management Framework (RMF) Implementation Procedures to cite this requirement. ECD: December 31, 2019.

Appendix XXII: Comments from the Small Business Administration



U.S. Small Business Administration

Office of the Chief Information Officer

Recommendation 59: The Administrator of the Small Business Administration should establish a process for conducting an organization-wide cybersecurity risk assessment.

SBA Response: Concur. The SBA is finalizing its process for conducting an enterprise-wide cybersecurity risk assessment. ECD: March 31, 2020.

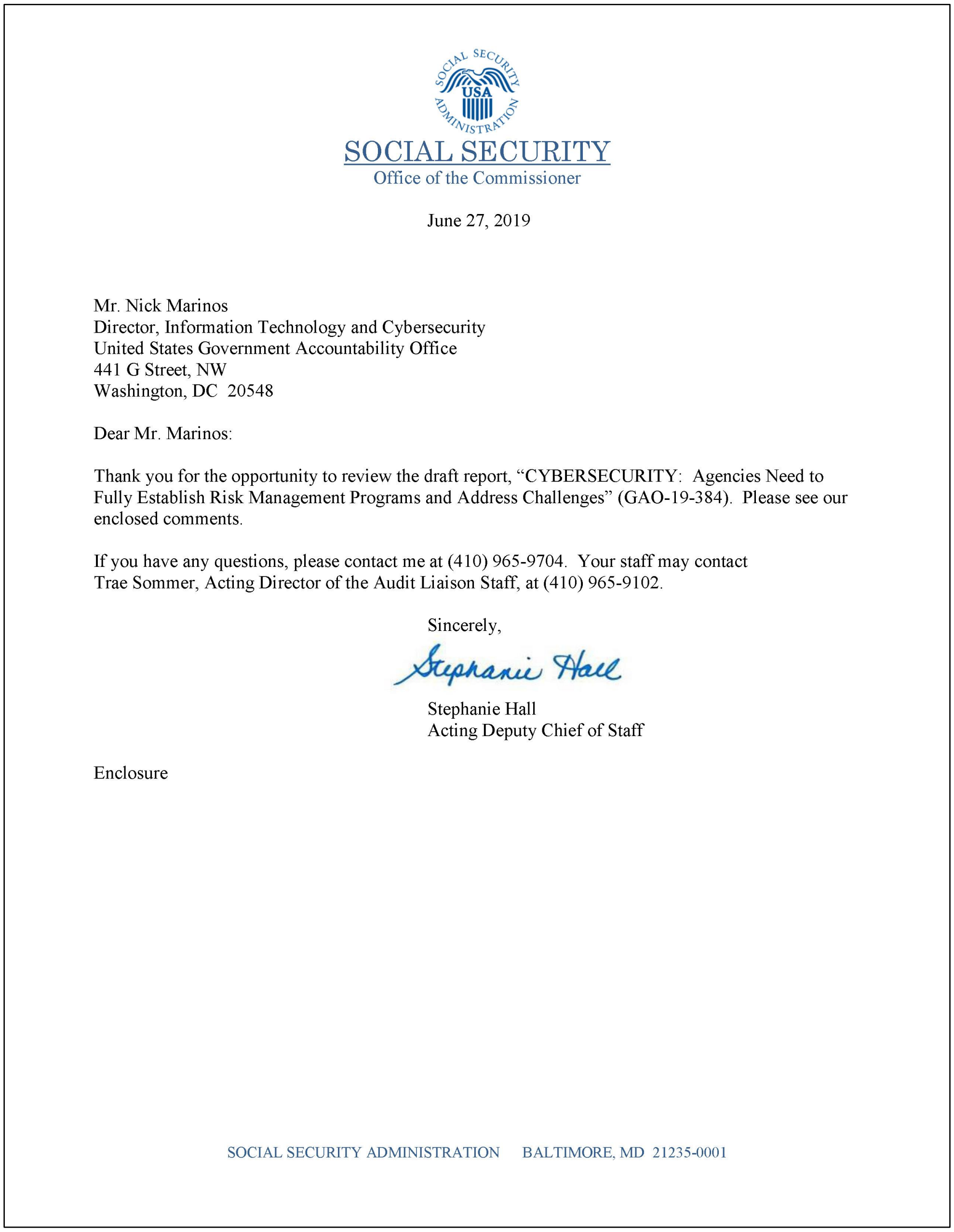
Thank you for the opportunity to comment on this draft report. SBA appreciates GAO's consideration of our comments prior to publishing the final report.

Sincerely,

MARIA ROAT Digitally signed by MARIA ROAT Date: 2019.07.11 16:34:28 -04'00'

Maria A. Roat
Chief Information Officer

Appendix XXIII: Comments from the Social Security Administration



SOCIAL SECURITY
Office of the Commissioner

June 27, 2019

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review the draft report, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges" (GAO-19-384). Please see our enclosed comments.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

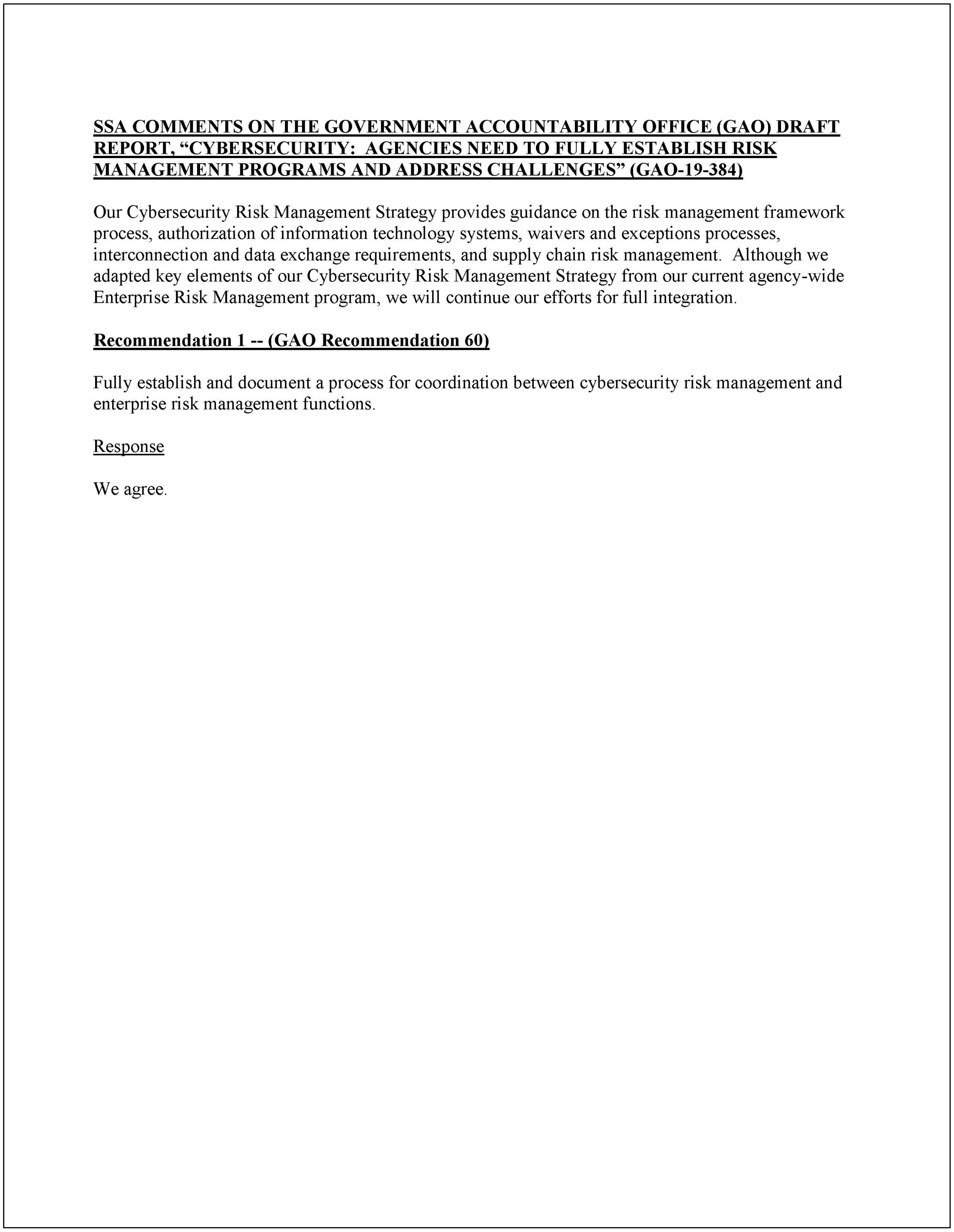
Sincerely,

Stephanie Hall

Stephanie Hall
Acting Deputy Chief of Staff

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001



SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES" (GAO-19-384)

Our Cybersecurity Risk Management Strategy provides guidance on the risk management framework process, authorization of information technology systems, waivers and exceptions processes, interconnection and data exchange requirements, and supply chain risk management. Although we adapted key elements of our Cybersecurity Risk Management Strategy from our current agency-wide Enterprise Risk Management program, we will continue our efforts for full integration.

Recommendation 1 -- (GAO Recommendation 60)

Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Response

We agree.

Appendix XXIV: GAO Contact and Staff Acknowledgments

GAO Contact

Nick Marinos, (202) 512-9342, marinosn@gao.gov

Staff Acknowledgments

In addition to the individual named above, Marisol Cruz Cain (assistant director), Lee McCracken (analyst in charge), Kiana Beshir, Roger Bracy, Chris Businsky, Alan Daigle, John de Ferrari, Nancy Glover, Franklin Jackson, Vernetta Marquis, Carlton Maynard, Scott Pettis, Tomas Ramirez, Andrew Stavisky, and Shaunyce Wallace made significant contributions to this report.

Appendix V: Accessible Data

Agency Comment Letter

Text of Appendix VIII: Comments from the Department of Education

Page 1

June 28, 2019

Ms. Carol Harris
Director, Information Technology Management Issues Information Technology and Cybersecurity Team
U.S. Government Accountability Office 441 G Street, NW
Washington, DC 20548

Dear Ms. Harris:

I am pleased to provide the U.S. Department of Education's (Department's) response to the Government Accountability Office's (GAO's) draft report, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges, GA0-19-384. We understand GAO conducted this audit to review federal agencies' cybersecurity risk management programs.

The Department concurs with GAO's recommendation and will continue necessary efforts to fully develop a cybersecurity risk management strategy that includes the definition of risk tolerance and acceptable risk response strategies.

You may direct your questions to Mr. Steven Hernandez, Chief Information Security Officer, Office of the Chief Information Officer, at (202) 245-7779 or at Steven.Hemandez@ed.gov.

Sincerely,

Jason K. Gray

Text of Appendix IX: Comments from the Department of Energy

Page 1

July 09, 2019

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Marinos:

The Department of Energy (DOE or Department) appreciates the opportunity to provide a management response to the Government Accountability Office's (GAO) draft report titled, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GA0-19-384). GAO conducted this audit to examine: (1) the extent to which agencies established key elements of a cybersecurity risk management program; and (2) what challenges, if any, the agency identified in developing and implementing cybersecurity risk management programs.

The draft report contained a total 60 recommendations, of which GAO directed two recommendations to DOE. DOE concurred with each of GAO's recommendations. Details are in the attached enclosure.

GAO should direct any questions to Emery Csulak, Office of Cybersecurity, Office of the Chief Information Officer (OCIO), via e-mail at Emery.Csulak@hg.doe.gov .

Sincerely,

Stephen (Max) Everett
Chief Information Officer

Enclosure

Page 2

MANAGEMENT RESPONSE
GAO Draft Report, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GA0-19-384)

Recommendation 8:

Develop a cybersecurity risk management strategy that includes the key elements identified in the report.

Management Decision: Concur

On May 15, 2019, the Department published DOE Order (0) 205.IC, Department of Energy Cybersecurity Program. The Order establishes the key elements for implementing risk management activities and guiding risk-based decisions identified by GAO in this report. Implementation of the Order will satisfy Recommendation 8. Specifically, the Order -

- Establishes cybersecurity roles and responsibilities, including the Cybersecurity Risk Executive for executing the risk management framework;
- Requires an Department-wide risk management plan in the form of an annual Enterprise Cybersecurity Program Plan (E-CSPP);
- Requires documented risk management plans from each Departmental Element (DE);
- Supports enterprise strategies for identification and monitoring of common controls;
- Requires periodic Department-wide cybersecurity risk assessments and management, review, and update of risk registers and documentation;
- Mandates system-level risk assessment to inform tailoring of controls and mitigation of weaknesses through plans of action and milestones (POA&Ms); and
- Requires risk-informed decisions about the operation and use of information systems.

DOE O 205.IC, as part of the E-CSPP, requires an Enterprise Cybersecurity Risk Management Strategy. The Strategy will delineate the Department's methodology for implementing the Order and define a

Departmental approach to framing, assessing, monitoring, and responding to risk in context of mission performance and assurance. Also, the Strategy will support DEs in making informed cybersecurity risk decisions, managing risk, and incorporating qualitative and quantitative approaches to risk assessment. Alignment and execution of the requirements of the Order, including creation of the E-CSPP, are required by May 2020.

Estimated Completion Date: May 31, 2020

Recommendation 9:

Update the Department's policies to address an organization-wide cybersecurity risk assessment and the identification of common controls.

Management Decision: Concur

Page 3

Federal government information systems and controls require approved information security plans. In May 2019, the Department published DOE O 205.IC, Department of Energy Cybersecurity Program. This Order presents a shared, distributed enterprise risk management approach to protect DOE information systems, comply with the Federal Information Security Modernization Act of 2014 (FISMA), and align with National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) risk assessment and management direction. The DOE Cybersecurity Program approaches implementation of cybersecurity requirements commensurate with impact to mission, national security, risk, and magnitude of harm. The Order requires development of a cybersecurity risk management strategy and approach, to include periodic risk assessments, based on aggregated information from system-level risk assessment, continuous monitoring, and mission-based risk considerations, and the quarterly review and update of risk registers.

DOE provides Departmental Elements with programmatic and operational flexibility to tailor and implement cybersecurity mitigation controls, based on risk assessments and in consideration of threats, mission needs, and environmental and operational factors. The Order also requires the Department to identify, document, publish, and monitor common controls for inheritance by multiple information systems, in accordance with NIST Special Publication (SP) 800-37, Rev 2, Risk Management Framework for

Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

The Department considers this recommendation closed.

Estimated Completion Date: DOE completed this action on May 15, 2019.

Text of Appendix X: Comments from the Department of Health and Human Services

Page 1

July 3, 2019

Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Marinos:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges" (GAO-19-384).

The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Sarah Arbes
Acting Assistant Secretary for Legislation

Attachment

Page 2

The U.S. Department of Health & Human Services (HHS) appreciates the opportunity from the Government Accountability Office (GAO) to review and comment on this draft report.

HHS leverages an enterprise risk management (ERM) approach to implement an enterprise-wide cybersecurity program to protect its critical in formation. HHS continuously monitors for new risks, prioritizes based on impact, and adjusts remediation and mitigation strategies. HHS continues to institutionalize cybersecurity as a key priority and enterprise issue, and has also ensured that cybersecurity and privacy risks are captured and addressed within HHS' enterprise- wide risk portfolio. HHS has established ERM to promote a risk-aware culture; drive strategic decision via agency risk; and establish and communicate risk appetite. The ERM Council - governed by the HHS Management Council - leads and oversees ERM across HHS. These governing bodies are part of HHS' Internal Governance Board that manages risk across HHS.

Additionally, HHS is working actively with a broad coalition of partners to enhance cybersecurity within the agency and across the Healthcare and Public Health Sector. HHS continues to work across the sector to raise awareness of the cybersecurity threats and tackle the shared challenges collaboratively. HHS is committed to the security and resiliency of the agency and the healthcare community.

Recommendation 10

The Secretary of Health and Human Services should:

- Develop a cybersecurity risk management strategy that include the key elements identified in this report.

HHS Response

HHS concurs with GAO's Recommendation 10.

- There are many federal-wide and HHS-specific initiatives that will help to operationalize HHS' Risk Management approach and strategy, which was shared with GAO.
- HHS will continue the deployment and implementation of a centralized, comprehensive security governance, risk, and compliance, reporting, and tracking tool (sGRC Archer) to enhance risk visibility and reporting at the Department-level. This will enable the development of an agency risk tolerance approach that is appropriate and feasible for HHS' federated environment 1; assessment of risk; determination of risk response strategies; and continuous monitoring of risk agency-wide.

- HHS will continue to work with OHS and integrators on the DHS CDM Program tool implementation, after which HHS anticipates increased enterprise environment visibility.

Page 3

- HHS will continue co-chairing the Cyber-ERM Community of interest with NIST. This group is a community of federal ERM and IT practitioners seeking to bridge communications across agency-level ERM and cybersecurity risk management functions.
- HHS will prioritize implementing and operationalizing HHS' cybersecurity risk management approach and strategy within the HHS HVA Program, consistent with current mandates and requirements, to inform risk management activities organization- wide. This includes informing leadership of the HHS HVA landscape, trends, opportunities and challenges, and possible security risks that could impact the enterprise and enable informed risk-based decisions.

Recommendation 11

The Secretary of Health and Human Services should:

- Update the department's policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform security control tailoring.

HHS Response

HHS concurs with the first part of Recommendation 11 regarding organization-wide cybersecurity risk assessment.

- HHS will continue the deployment and implementation of a centralized, comprehensive security governance, risk, and compliance, reporting, and tracking tool (sGRC Archer) to enhance risk visibility and reporting at the Department-level. This will enable the development of an agency risk tolerance approach that is appropriate and feasible for HHS' federated environment; assessment of risk; determination of risk response strategies; and continuous monitoring of risk agency-wide.
- HHS will continue to work with DHS and integrators on the DHS CDM Program tool implementation, after which HHS anticipates increased enterprise environment visibility. We are also complementing this

CDM deployment with other tools to ensure we have a near real-time understanding of the most critical cybersecurity vulnerabilities to the agency and that we can share this information quickly with those who can best address those vulnerabilities.

HHS non-concurs with the second part of Recommendation 11 regarding the use of risk assessments to inform security control tailoring. The GAO Statement of Facts (page 13) also stated that "... HHS... have a policy that calls for risk assessments to inform the tailoring of security controls..." The reasons for non-concurring are the following:

- The HHS Information System Security and Privacy Policy (IS2P), updated through an addendum on May 24, 2018, establishes comprehensive IT security and privacy requirements for the IT security programs and information systems of Op Divs and Staff Divs. The IS2P, which complies with the requirements of the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision 4, requires the use of risk assessments to inform and guide the selection of security controls.

Page 4

- The selection of security, privacy and common controls is addressed in each system security plan (SSP)/Privacy Plan and the IS2P. According to the IS2P, each system is required to have an SSP. In addition, HHS policy requires the use of a risk assessment when selecting and tailoring security controls. Pertinent sections of the IS2P are as follows:
    - Section 4.1, Department-Mandated Controls, requires "the use of NIST SP 800- 37, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, as the methodology for the security assessment and authorization (SA&A) of information systems ... in accordance with FISMA and direction from the Office of Management and Budget (OMB)."
    - Section 4.1.2 states "OpDivs/StaffDivs must ensure that information systems provide adequate, risk-based protection in the control areas defined in the Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, by using the appropriate baseline security controls as established in NIST SP 800-53, Recommended Security Controls for Federal Information

Systems, in accordance with the impact level for the system as defined in FIPS 199, Standards for Security Categorization of Federal Information and Information Systems."

  - o Appendix B, PL-2 #8 and #9 states "Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions" and "Is reviewed and approved by the authorizing official or designated representative prior to plan implementation".

- The HHS Waiver/Risk Acceptance Guidance/Template provides guidance for documenting and managing accepted risks. Also, the HHS Plan of Action and Milestones Standard includes the requirements for documenting, remediating, mitigating, and monitoring of vulnerabilities, weaknesses, and other risks. It is important to note that these risk-based decisions are performed at the OpDiv-level, consistent with the HHS CIO delegation of authority to OpDiv CIOs (footnote 2). An HHS division is best- positioned to understand its IT environment, the impacts of risks posed to that environment, and the resources available to implement and act upon such risk-based decisions.

Recommendation 12

The Secretary of Health and Human Services:

- Establish a process for conducting an organization-wide cybersecurity risk assessment.

HHS Response

HHS concurs with GAO's Recommendation 12.

- HHS will continue the deployment and implementation of a centralized, comprehensive security governance, risk, and compliance, reporting, and tracking tool (sGRC Archer) to…

Text of Appendix XI: Comments from the Department of Homeland Security

Page 1

June 28, 2019

Nick Marinos
Director, Information Technology & Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-19-384, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges"

Dear Mr. Marinos:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

We are pleased to note GAO's positive recognition of the Office of Management and Budget and DHS' work to identify areas for improvement in agencies' capabilities for managing cyber risks including:

- Using the metrics collected during the "Federal Information Security Modernization Act of 2014" (FISMA) reporting process to update each agency's risk management assessment on an ongoing basis, and
- Taking steps to align government wide cybersecurity guidance with the National Institute of Standards and Technology framework, such as updating the reporting guidance on chief information officer and Inspector General FISMA metrics to align with the framework.

DHS agrees with GAO that "given the increasing number and sophistication of cyber threats facing federal agencies, it is critical that agencies are well positioned to make consistent, informed risk-based decision in protecting their systems and information against these threats." DHS is committed to continuously reviewing and improving its existing processes and procedures to better coordinate information security risks with the enterprise risk management functions and aligning cybersecurity risk within the Department's risk tolerance determinations.

Page 2

The draft report contained sixty recommendations, including two for DHS with which the Department concurs. Attached find our detailed response to each of these recommendation. Technical comments were previously provided under separate cover.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations Contained in GA0-19-384

GAO recommended that the Secretary of Homeland Security:

Recommendation 14:

Develop a cybersecurity risk management strategy that includes the key elements identified in this report.

Response: Concur. The DHS Office of the Chief Information Officer (OCIO), Chief Information Security Officer (CISO), will review and enhance the Department's existing cybersecurity risk program and strategy by ensuring that (1) FISMA tracking and compliance activities, (2) the implementation of Continuous Diagnostic and Mitigation, (3) Agency-Wide Adaptive Risk Enumeration (AWARE) risk methodology results, and (4) cybersecurity risk management policy requirements are incorporated, as appropriate. This will further enhance the existing cybersecurity risk management program and strategy and improve the integration of cybersecurity risk with the Department's enterprise risk management program. Estimated Completion Date (ECD): July 31, 2020.

Recommendation 15:

Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Response: Concur. The CISO, in conjunction with other OCIO staff, such as the Cybersecurity Solutions Division, will facilitate enhancements to existing policy, further clarifying the cybersecurity risk executive's role at both the Headquarters and Component levels, and enhancing requirements to integrate cybersecurity risks into existing enterprise risk management activities. ECD: July 31, 2020.

Text of Appendix XII: Comments from the Department of Housing and Urban Development

Page 1

July 3, 2019

Mr. Lee McCracken
Senior Analyst, IT
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. McCracken:

Thank you for the opportunity to review and comment on the draft report for GAO-19-384, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges. The U.S. Department of Housing and Urban Development has no comments on the report and concurs with the recommendations.

If you have questions or require additional information, please contact Janice Ausby, Deputy Chief Information Officer, Business and IT Resource Management Office, at (202) 402-7605 (Janice. L.Ausby@hud.gov), or Juanita L. Toatley, Audit Liaison, Audit Compliance Branch, at (202) 402-3555 (Juanita.L.Toatley@hud.g ov).

Sincerely,

David Chow
Chief Information Officer

Page 2

cc:

Kevin R. Cooke, Jr., Principal Deputy Chief Information Officer, Q

Janice (Ausby) Boyd, Deputy CIO for Business and IT Resource Management, QRM Sheron Parker, Director, Financial Administrative Specialist, OCIO, QREA

Nathan Merritt, Director, Office of Systems Integration and Efficiency, OCIO, QRE Wynee Watts-Mitchell, Director, Audit Compliance Branch, OCIO, QMAC

Juanita Toatley, IT Specialist, Audit Compliance Branch, OCIO, QMAC

Helen McBride, Senior Advisor to the Principal Deputy Chief Information Officer, Q Michael A. Simms, Administrative Officer, Administrative Services Branch, OCIO, QMAS Steven J. Parker, Jr., Management Analyst, Administrative Services Branch, OCIO, QMAS Oscar V. Franklin, Director, Audit Liaison Division, OCFO, FMA

Text of Appendix XIII: Comments from the Department of the Interior

Page 1

July 1, 2019

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington; DC 20548

Dear Mr. Marinos:

Thank you for providing the Department of the Interior (Department) the opportunity to review and comment on the draft U.S. Government Accountability Office (GAO) report entitled, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384). We appreciate GAO's review of the Department's cybersecurity risk management program.

GAO issued the Department three recommendations to address its findings. Below is a summary of actions planned or taken to implement the recommendations.

Recommendation 18:

Develop a cybersecurity risk management strategy that includes the key elements identified in this report.

Response: Concur. The Department has assigned a Cybersecurity Risk Executive in the Office of the Chief information Officer (OCIO) and developed an overarching framework for cybersecurity risk management. The Department will evaluate the current environment to ensure its cybersecurity risk management strategy is carried out at the correct level in the Department, with agency-wide oversight of cybersecurity risk activities and adequate resources to carry out appropriate actions across the Department. The Department will develop and implement the cybersecurity risk management strategy in coordination with the Cybersecurity Risk Executive, within the framework for cybersecurity risk management that includes a statement of risk tolerance; risk assessment approach; acceptable risk response strategies; and monitoring risks over time.

Recommendation 19:

Update the department's policies to address an organization-wide cybersecurity risk assessment.

Response: Concur. The Department will establish a cybersecurity risk management strategy that reflects risk tolerance and a process to aggregate and evaluate agency wide risks. The Department will create policies in coordination with the cybersecurity risk executive function to specify key roles across the agency, including implementing agency-wide cyber risk assessments that are monitored and reported on an ongoing basis, as defined in the cybersecurity risk management strategy.

Page 2

Recommendation 20: Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Response: Concur. The Cybersecurity Risk Executive will inform the Department's enterprise risk management officials about cybersecurity risks that are to be considered when making operational, legal, strategic, and capital planning as well as other management decisions. Across the Department, programs must effectively identify, assess, and prioritize actions to mitigate cybersecurity risks in the context of other enterprise risks.

If you have any questions or need additional information, please contact William Vajda, Chief Information Officer at william_vajda@ios.doi.gov, or the OCIO audit liaison Richard Westmark at richard_westmark@ios.doi.gov.

Sincerely,

Scott J. Cameron
Principal Deputy Assistant Secretary for Policy, Management and Budget

Text of Appendix XIV: Comments from the Department of Labor

Page 1

June 21, 2019

Mr. Nick Marinos
Director, Information Technology And Cybersecurity
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for the opportunity to review and comment on draft report GAO-19-384 Cybersecurity: Agencies Need to Fully Establish Risk

Management Programs and Address Challenges. We appreciate the Government Accountability Office's (GAO) efforts and insights.

Recommendation 24:

The Secretary of Labor should update the department's policies to address the use of risk assessments to inform control tailoring and POA&M prioritization.

DOL Response: DOL concurs with the draft GAO recommendation. The Department will take the necessary steps to update the department's policies to address the use of risk assessments to inform control tailoring and POA&M prioritization.

Should you have any questions regarding the Department's response, please have your staff contact Gundeep Ahluwalia, Chief Information Officer, at (202) 693-4200.

Sincerely,

Bryan Slater
Assistant Secretary for
Administration and Management

Text of Appendix XV: Comments from the Department of State

Page 1

July 2, 2019

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

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges" GAO Job Code 102633.

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

Sincerely,

Jeffrey C. Mounts (Acting)

Enclosure:
As stated

cc: GAO - Nick Marinos
IRM - Stuart McGuigan
OIG - Norman Brown

Page 2

Department of State Response to the Draft Report

CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges
(GAO-19-384, GAO Code 102633)

Thank you for the opportunity to Comment on the GAO draft report

“Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges.”

Recommendations 25 & 26:

The Secretary of State should: Update the department’s policies to address an organization-wide risk assessment, an organization-wide strategy for monitoring control effectiveness, system-level risk assessments, the use of risk assessments to inform security control tailoring, and the use of risk assessments to inform POA&M prioritization. (25) Establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions. (26)

Response:

The Department concurs with the recommendations, and is actively working on updating the applicable policies and procedures to integrate risk at all three levels—organization, bureau, and information systems—into the Department's Information Security Program (ISP).

To further align with federal requirements and guidelines, the Department established the Cyber Risk Management program at the end of FY18 to implement a Department-wide cyber risk management strategy. This program will also coordinate the updates to the Department's policies to address the risk-based policy gaps identified during GAO's review. The following policy updates are currently in progress and will be submitted for internal review and approval by September 2020.

- The Department is developing Department-wide (Tier 1) risk assessment policies and procedures that align with both NIST SP 800-39 and the Department's Enterprise Risk Management (ERM) program. The assessment at the Department-level will focus more on ISP efforts and significant system vulnerabilities identified in an IT system that is in use across the enterprise.

Page 3

- The Department is updating its policies to ensure compliance, its effectiveness, and monitor changes that can alter the parameters of what was previously acceptable risk. Control monitoring should also be aligned to the tier where the risk response occurred. The Department has mechanisms and governance activities focused on risk monitoring. At the system tier, the Department uses monitoring tools capable of evaluating the cybersecurity capabilities of its systems and their environment of operation. Similar capabilities are being configured and employed for cloud environments and are being augmented with the implementation of Continuous Diagnostics and Mitigation tools from the Department of Homeland Security. Regardless of the tool, where possible, these monitoring capabilities are being configured to consider system categorization levels and Department risk thresholds to support automated risk monitoring and alerting.

- The Department is updating its policies to ensure risk assessments are always conducted and updated on an ongoing basis. The Department's risk assessment policies will focus on the likelihood of an event occurring that would have an adverse effect. This effect would be considered differently at each tier yet remain focused on the use of IT. Cyber threat intelligence characterization information is pulled from DS/CTS into the assessment process. Risks identified and assessed against systems will be tracked and managed through the NIST RMF process. Risks not directly attributable to a system or systems will be tracked and monitored in a separate risk register. As appropriate and in accordance with ERM policies, certain risks will populate the enterprise risk profile.

- The Department is updating its internal risk management framework (RMF) policies and process to ensure the selection of controls arrive at the appropriate risk tolerance levels established in collaboration with the Department's enterprise risk management (ERM) efforts, and that such are tailored to accurately represent the organizational information systems and environments of operations.

In addition to these policy updates, the Department is working diligently to align the cyber risk management program with the ERM governance structure. In July 2018, the Department established the Enterprise Risk Management Council (ERMC) in accordance with OMB Circular A-123, chaired by the Deputy Secretary and comprised of all six Under Secretaries. The ERMC is supported by the Office of Management Policy, Rightsizing, and Innovation (M/PRI) acting as the secretariat as well as the ERM program office. M/PRI created and maintains an enterprise risk profile, which has been reviewed by the ERMC. The enterprise risk profile includes enterprise-level cybersecurity risks. While the Department's

Text of Appendix XVI: Comments from the Department of Veterans Affairs

Page 1

July 8, 2019

Mr. Nick Marinos
Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

The Department of Veterans Affairs ,YA) has reviewed the Government Accountability Office (GAO) draft report: CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384).

The enclosure sets forth the actions to be taken to address the draft report recommendations.

VA appreciates the opportunity to comment on your draft report.

Sincerely,

Robert L. Wilkie
Enclosure

Page 2

VA Recommendation 1:

The Secretary of Veterans Affairs should develop a cybersecurity risk management strategy that includes the key elements identified in this report. (Report Recommendation 34).

VA Comment: Concur. The Department of Veterans Affairs (VA) Risk Management Framework (RMF) tracks emerging risk requirements (executive orders, updates to National Institute of Standards and Technology, etc.) and develops processes for VA to implement those requirements across the organization. The RMF takes a risk-based approach to reviewing, prioritizing, and addressing new compliance regulations.

VA developed a risk profile that prioritizes risks that are significant threats to the accomplishment of VA's mission and objectives, as determined by VA's Office of Information and Technology (OIT) leadership. The risk profile facilitates open dialogue about risks among OIT leadership and allows VA to continuously monitor and prioritize mitigation of risks based on the impacts to VA. VA continues to develop and refine risk management processes in order to drive improvement and reduce deficiencies.

VA continues to implement the above processes into an organization-wide risk management strategy that will incorporate the items outlined in the Government Accountability Office (GAO) report: (1) a statement of the agency's risk tolerance; (2) how VA intends to assess risk; (3) acceptable risk response strategies; and (4) how the agency intends to monitor risk over time. VA will provide more detailed information regarding implementation in our 180-day update to GAO's final report. Target Implementation Date: December 31, 2019.

VA Recommendation 2:

The Secretary of Veterans Affairs should update the department's policies to address an organization-wide cybersecurity risk assessment (Report Recommendation 35).

VA Comment: Concur. VA will incorporate into Department policies the requirement for completing, updating, and documenting an agency-wide assessment of cybersecurity risk. VA will provide more detailed information regarding implementation in our 180-day update to GAO's final report. Target Implementation Date: December 31, 2019.

VA Recommendation 3:

The Secretary of Veterans Affairs should establish a process for conducting an organization-wide cybersecurity risk assessment (Report Recommendation 36).

VA Comment: Concur. VA defines risk assessment processes at the mission/business and information system levels and is further advancing its capabilities to establish an Enterprise Risk Management process consistent with the Federal

Page 3

Information Security Modernization Act (42 United States Code 3554). VA will provide more detailed information regarding implementation in our 180-day update to GAO's final report. Target Implementation Date: June 30, 2020.

VA Recommendation 4:

The Secretary of Veterans Affairs should establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions (Report Recommendation 37).

VA Comment: Concur. VA has established a governance structure that allows for reporting and coordination between cybersecurity risk management and enterprise risk management functions. VA's RMF process standardizes the management of identified enterprise risks, and evaluates VA's IT assets and resources across the organization.

Through the VA RMF, VA leverages governance reporting processes to provide executive leadership with a centralized and transparent view of VA cybersecurity projects and initiatives. Governing bodies have been established from the executive level through the implementation/operational level to identify, track, and coordinate on topics regarding cybersecurity risk management and enterprise risk management. The appropriate governing bodies have been established addressing the recommendation.

VA OIT's governance bodies such as the Standards and Architecture Council (SAC), chaired by VA's Chief Information Security Officer, review and approve policies, rules, standards, and content that affects the current and future states of VA's technologies. The SAC's subcommittees, such as the Information Security Committee, allow for an integrated viewpoint of the strategic, operational, and external risks the organization is facing. To support the advancement of VA's policies and procedures as well as the maturation of its cybersecurity environment, OIT established the RMF Technical Advisory Group (RMF TAG). The SAC was established in October 2018; the ISC was established in June 2018; and the RMF TAG was established in February 2019. AU three of the committees meet on a monthly cadence.

The VA OIT Enterprise Cybersecurity Program (ESCP) Concept of Operations (CONOPS) and ECSP Governance Framework Charter describe in detail the governance structure referenced above. The CONOPS and Charter are attached as supporting documentation (Attachments A and B); both documents have been approved internally and are pending final publication.

Based on the defined structure and communication channels in place, VA senior leadership plays a direct role in the implementation of VA's cybersecurity risk management strategy and ongoing integration efforts across the enterprise. This direct engagement provides Department leadership with a continual understanding of VA's cybersecurity risks, positioning them to make informed decisions in support of risk reduction for the Department. OIT requests closure of the recommendation based on the actions described above.

Text of Appendix XVII: Comments from the U.S. Agency for International Development

Page 1

Nick Marinos
Director,
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

Re: CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384).

Dear Mr. Marinos:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability office (GAO) titled, CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384).

USAID is committed to improving our management of risks associated with the operation and use of information systems that support our mission and business functions. The GAO acknowledges that USAID is one of only seven of the 23 civilian Departments and Agencies covered by the Chief Financial Officers Act that has developed a cybersecurity risk-management strategy that fully addresses the four elements established in Special Publication (SP) 800 39, Managing Information Security Risk: Organization, Mission, and Information System View, issued by the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce. Specifically, the GAO found that-USAID has developed a strategy to guide how to frame, assess, respond to, and monitor cybersecurity. At the same time, USAID acknowledges improvements we must make to continue managing cybersecurity risks carefully.

USAID is updating our policies to conduct an organization-wide cybersecurity risk- assessment and also use risk-assessments to inform control-tailoring. Our Chief Information Officer has developed and documented the USAID Security Assessment and Authorization (SA&A)

Process, which established Agency-wide roles, responsibilities, and procedures to implement the NIST Risk-Management Framework. The SA&A Process informs work flows .that should ensure senior USAID executives are explicitly aware of the operational risks they accept through the implementation and use of information systems. This construct allows the Agency to prioritize and categorize our critical assets, identify associated systemic weaknesses and security flaws, and build strategies to mitigate cyber-related risk through a consistent approach. In addition, USAID is further amending our policies to include specific processes for an organization-wide cybersecurity risk-assessment and how to use the results of such an evaluation to strengthen our control-tailoring process even further.

Page 2

USAID appreciates this opportunity to provide documentation of our compliance with the goals and standards set by the Office of Management and Budget (OMB) and the U.S. Department of Homeland Security (DHS). USAID's Agency Risk Profile, issued in June 2018, includes cybersecurity risks reported at the enterprise level. We continually update the Risk Profile, and evaluate additional cybersecurity risks to ensure appropriate organization-wide coverage is ongoing. In addition, USAID became the first Federal Agency to publish a Risk-Appetite Statement, available on our public website at https//www.usaid.gov/sites/default/files/documents/1868/USAID_Risk-Appetite-Statement-Jun2018.pdf, which expresses our clear intolerance for cybersecurity breaches.

I am transmitting this letter and the enclosed comments from USAID for inclusion in the GAO's final report. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement. We appreciate the opportunity to participate in the complete and thorough evaluation of our cybersecurity risk-management program and practices.

Sincerely,

Angelique M. Crumbly
Senior Deputy Assistant Administrator
Bureau for Management

Enclosure: a/s

Page 3

COMMENTS BY THE U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT ON THE DRAFT REPORT PRODUCED BY THE U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO) TITLED, CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GA0 -19-384)

The U.S. Agency for International Development (USAID) would like to thank the U.S. Government Accountability Office (GAO) for the opportunity to respond to this draft report. We appreciate the extensive work of the GAO engagement team and the specific findings that will help USAID achieve greater effectiveness in our cyber security risk-management.

Information technology (IT) is interwoven into all aspects of USAID operations, and is among the most vital investments that support the Agency's work all around the world. The IT landscape continues to evolve at a rapid pace, arid technological advances provide opportunities· for USAID to operate more efficiently and effectively, At the same time, cyber threats continue· to grow in aggressiveness and sophistication, as the Agency’s need to share and use information grows. We recognize the important role IT plays in supporting our mission and are committed to delivering robust, responsive, and flexible IT services and products, while protecting information and information systems from security threats.

The draft report contains two recommendations for USAID. ·The Agency agrees with both recommendations, and is already addressing them.

1. The Administrator of USAID should update the agency's policies to address an organization-wide cybersecurity risk-assessment and the use of risk-assessments to inform control -tailoring.

USAID's Chief Information Office in the Bureau for Management (M/CIO) has developed and documented the USAID Information-Technology (1T.) Systems Risk-Management Framework (RMF) Handbook, which defines Agency-wide roles, responsibilities, and procedures for the implementation of the RMF issued by the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce. .The Handbook suppo1is security assessment and authorization (SA&A) for information systems a4d system connections, and describes multiple SA&A workflows that ensure senior USAID executives are explicitly aware of the operational risks they are accepting through the implementation and use of information systems.

Text of Appendix XVIII: Comments from the General Services Administration

Page 1

July 5, 2019

The Honorable Gene L. Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the Government Accountability Office's draft report titled CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges (GAO-19-384).

The report contains 4 recommendations addressed to the Administrator of General Services:

- Designate and document a risk executive function with responsibilities for organization- wide cybersecurity risk management (Recommendation 44).
- Update the agency's policies to address an organization-wide cybersecurity risk assessment (Recommendation 45).
- Establish a process for conducting an organization-wide cybersecurity risk assessment (Recommendation 46).
- Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions (Recommendation 47).

GSA concurs with the findings in the draft report and is implementing an action plan to address the recommendations.

If you have any questions, please contact me at (202) 969-7277 or Jeffrey Post, Associate Administrator, Office of Congressional and Intergovernmental Affairs, at (202) 501-501-0563.

Sincerely,

Emily W. Murphy
Administrator

Text of Appendix XIX: Comments from the National Aeronautics and Space Administration

Page 1

July 1, 2019

Reply to Attention of: Office of the Chief Information Officer

Mr. Nick Marinos
Director
Information Technology and Cybersecurity
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Marinos:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges," (GAO-19-384), dated June 3, 2019.

In the draft report, GAO makes two recommendations to NASA intended to improve the Agency's cybersecurity risk assessment policy and processes. Specifically, GAO recommends the following:

Recommendation 1:

Update the agency's polices to require (1) conducting an organization-wide cybersecurity risk assessment and (2) the use of risk assessments to inform plan of action and milestones (POA&M) prioritization.

Management's Response: Concur. NASA will update its relevant policies to require:

(1) conducting an organization-wide cybersecurity risk assessment and
(2) the use of risk assessments to inform POA&M prioritization.

Estimated Completion Date: September 30, 2020

Recommendation 2:

Establish a process for conducting an organization-wide cybersecurity risk assessment.

Management's Response: Concur. NASA will document its process for conducting an organization-wide cybersecurity risk assessment.

Estimated Completion Date: September 30, 2020

Page 2

We have reviewed the draft report for information that should not be publicly released. As a result of this review, we have not identified any information that should not be publicly released.

Once again, thank you for the opportunity to comment on the subject draft report. If you have any questions or require additional information, please contact Ruth McWilliams on (202) 358-5125.

Sincerely,

Renee P. Wynn
Chief Information Officer

Text of Appendix XX: Comments from the Nuclear Regulatory Commission

Page 1

July 3, 2019

Nick Marinos, Director
Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Marinos:

Thank you for giving the U.S. Nuclear Regulatory Commission (NRC) the opportunity to review and comment on the U.S. Government Accountability Office's (GAO's) draft report issued June 2019, GA0-19-384, "Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges." The NRC has reviewed the draft report and is in general agreement with its findings and recommendations.

If you have any questions on the NRC's response, please contact John Jolicoeur by phone at (301) 415-1642 or by e-mail to John.Jolicoeur@nrc.gov.

Sincerely,

Margaret M. Doane
Executive Director
for Operations

Text of Appendix XXI: Comments from the Office of Personnel Management

Page 1

July 3, 2019

Mr. Gregory C. Wilshusen
Director, Info1mation Security Issues

U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Subject: Agency Response to Draft Report for GAO-19-384, Job Code 102633

Dear Mr. Wilshusen:

Thank you for providing us the opportunity to respond to the Government Accountability Office (GAO) draft report, Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges, GAO-19-384, job code 102633. Responses to your recommendations are provided below.

Recommendation #55:

Update the agency's policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform control tailoring.

Management Response:

We concur. Our current processes for control tailoring include considerations for business impacts. Going forward, we plan to review and strengthen our existing policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform control tailoring, where appropriate.

Recommendation #56:

Establish a process for conducting an organization-wide cybersecurity risk assessment.

Management Response:

We concur. We plan to formalize our process for conducting an organization-wide cybersecurity risk assessment.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Chief Information Security Officer Cord Chase at 202-606-0117 or Cord.Chase@opm.gov.

Sincerely,

Clare A. Martorana
Chief Information Officer

Text of Appendix XXII: Comments from the Small Business Administration

Page 1

July 3, 2019

Mr. Nicholas Marinos
Director, Cybersecurity and Information Management Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Marinos:

Thank you for providing the U. S. Small Business Administration (SBA) with a copy of the Government Accountability Office (GAO) draft report titled “Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges”, GAO-19-384 (102633). The draft report analyzes the extent to which agencies have established key elements of a cybersecurity risk management program, what challenges they have discovered in establishing a cybersecurity risk management program, and steps OMB and DHS have taken to meet their risk management responsibilities.

The SBA has reviewed the draft report and agrees with the three recommendations identified in the draft report. Additional details are provided below:

Recommendation 57:

The Administrator of the Small Business Administration should fully develop a cybersecurity risk management strategy that includes the key elements identified in this report.

SBA Response: Concur. Although the SBA already developed a cybersecurity risk management strategy, SBA will more clearly articulate and enhance the strategy in the key areas of risk tolerance and risk mitigation strategies. Estimated completion Date (ECD): December 31, 2019.

Recommendation 58:

Administrator of the Small Business Administration should update the agency's policies to address an organization-wide cybersecurity risk assessment and the use of risk assessments to inform POA&M prioritization.

SBA Response: Concur. The SBA's practice is to prioritize its POA&Ms based on the risk impact assigned by the independent assessor. To fully address the recommendation, SBA will update our Risk Management Framework (RMF) Implementation Procedures to cite this requirement. ECD: December 31, 2019.

Page 2

Recommendation 59:

The Administrator of the Small Business Administration should establish a process for conducting an organization-wide cybersecurity risk assessment.

SBA Response: Concur. The SBA is finalizing its process for conducting an enterprise-wide cybersecurity risk assessment. ECD: March 31, 2020.

Thank you for the opportunity to comment on this draft report. SBA appreciates GAO's consideration of our comments prior to publishing the final report.

Sincerely,

Maria A. Roat
Chief Information Officer

Text of Appendix XXIII: Comments from the Social Security Administration

Page 1

June 27, 2019

Mr. Nick Marinos
Director, Information Technology and Cybersecurity
United States Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Marinos:

Thank you for the opportunity to review the draft report, "CYBERSECURITY: Agencies Need to Fully Establish Risk Management Programs and Address Challenges" (GAO-19-384). Please see our enclosed comments.

If you have any questions, please contact me at (410) 965-9704. Your staff may contact Trae Sommer, Acting Director of the Audit Liaison Staff, at (410) 965-9102.

Sincerely,

Stephanie Hall
Acting Deputy Chief of Staff

Enclosure

Page 2

SSA COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "CYBERSECURITY: AGENCIES NEED TO FULLY ESTABLISH RISK MANAGEMENT PROGRAMS AND ADDRESS CHALLENGES" (GAO-19-384)

Our Cybersecurity Risk Management Strategy provides guidance on the risk management framework process, authorization of information technology systems, waivers and exceptions processes, interconnection and data exchange requirements, and supply chain risk management.

Although we adapted key elements of our Cybersecurity Risk Management Strategy from our current agency-wide Enterprise Risk Management program, we will continue our efforts for full integration.

Recommendation 1 (GAO Recommendation 60)

Fully establish and document a process for coordination between cybersecurity risk management and enterprise risk management functions.

Response:

We agree.

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 GAO's website (https://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to https://www.gao.gov and select "E-mail Updates."

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 E-mail 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/fraudnet/fraudnet.htm

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

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