United States Government Accountability Office

Report to Congressional Committees

July 2022

COAST GUARD

Actions Needed to Enhance IT Program Implementation

Accessible Version

GAO Highlights

Highlights of GAO-22-105092, a report to congressional committees

July 2022

COAST GUARD

Actions Needed to Enhance IT Program Implementation

Why GAO Did This Study

The U.S. Coast Guard, a component of the Department of Homeland Security, relies extensively on IT systems and services to carry out its 11 statutory missions. It also relies on operational technology, which encompasses a broad range of programmable systems or devices that interact with the physical environment, such as sensors and radar. Historically, the Coast Guard has had longstanding issues managing its technology resources. As such, it plans to spend $93 million to improve the reliability and performance of these resources in fiscal year 2022.

The *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* included a provision for GAO to review several aspects of the Coast Guard's IT program. This report addresses, among other things, the extent to which the Coast Guard (1) has a process to plan for network capacity; (2) has cybersecurity risk management processes for IT and for operational technology; and (3) has incorporated federal requirements in its strategy for cloud computing.

To do so, GAO evaluated the Coast Guard's IT policies and procedures against common practices for network capacity planning. GAO also analyzed the Coast Guard's cybersecurity processes for IT and operational technology and assessed their application. Further, it assessed the cloud strategy and other related documentation against federal requirements and guidance.

What GAO Recommends

GAO is making eight recommendations to improve the Coast Guard's IT program implementation. The Department of Homeland Security agreed with all eight recommendations.

View GAO-22-105092. For more information, contact Jennifer R. Franks at (404) 679-1831 or FranksJ@gao.gov.

What GAO Found

The U.S. Coast Guard lacks a documented network capacity planning process. Network capacity planning is an important aspect of IT infrastructure planning that involves determining the network resources required to support an entity's mission. However, the Coast Guard uses an ad hoc process that does not fully align with five common practices GAO identified for network capacity. The table below describes the extent to which it implemented the practices. Without fully implementing these practices, the Coast Guard faces significant risks in resulting inefficiencies and disruptions in network availability to users.

Extent to Which Coast Guard Implemented Network Capacity Planning Practices

Common Practices	Implementation Status
Compile an inventory of hardware, software, and configurations	partially addressed
Identify the baseline network utilization and traffic growth predictions	partially addressed
Determine bandwidth allocation needs for variations and prioritize network traffic	partially addressed
Run simulations and perform analyses of network usage	Not addressed
Make refinements to the network and continually monitor the health of the infrastructure	partially addressed

Legend:
● = addressed: The Coast Guard demonstrated that it had fully implemented the practice; ◑ = partially addressed: The Coast Guard demonstrated that it implemented some, but not all of the practice; and ○= not addressed: The Coast Guard could not demonstrate that it had implemented the practice.

Source: GAO analysis of U.S. Coast Guard documentation and industry publications. | GAO-22-105092

In accordance with the January 2017 agreement between the Department of Homeland Security and Department of Defense (DOD), the Coast Guard is to follow DOD's Risk Management Framework. This framework establishes two different cybersecurity risk management processes for identifying and applying cybersecurity controls for IT and for operational technology resources. However, the Coast Guard did not consistently apply the framework for its operational technology. This inconsistency is due in part to the lack of a comprehensive and accurate inventory. In addition, it lacks a cybersecurity risk management process for two types of operational technology—industrial control systems and supervisory control and data acquisition systems. Without a consistently applied process, accurate inventory, and coverage for all systems, the Coast Guard cannot ensure effective management of cybersecurity risks.

In March 2021, the Coast Guard issued a cloud strategy that outlines its strategic objectives for cloud computing over the next five years. The cloud strategy and associated relevant documentation incorporated most federal cloud requirements and guidance. However, the Coast Guard did not address key actions related to security and its workforce. Updating its strategy to include all cloud-related requirements and guidance would further facilitate the migration to cloud services.

Contents

Tables

Figures

Abbreviations

C4&IT	Command, Control, Communications, Computers, and IT
C5I	Command, Control, Communications, Computers, Cyber, and Intelligence
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
DevSecOps	development, security, and operations
DHS	Department of Homeland Security
DOD	Department of Defense
ESI	Enterprise Systems Inventory
FedRAMP	Federal Risk and Authorization Management Program
FIPS 199	Federal Information Processing Standards 199
ICAM	Identity, Credential, and Access Management
ICS	industrial control system
MISLE	Marine Information for Safety and Law Enforcement
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIT system	platform information technology system
POA&M	plan of action and milestones
RMF	risk management framework
SCADA	supervisory control and data acquisition
SLA	service level agreements
SSP	system security plan

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

July 28, 2022

The Honorable Maria Cantwell
Chair
The Honorable Roger F. Wicker
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Peter A. DeFazio
Chairman
The Honorable Sam Graves
Ranking Member
Committee on Transportation and Infrastructure
House of Representatives

The U.S. Coast Guard—a component of the Department of Homeland Security (DHS)—is the principal federal agency responsible for maritime safety, security, and environmental stewardship in U.S. ports and waterways. It has responsibility for 11 statutory missions that include protecting and defending more than 95,000 miles of U.S. coastline and inland waterways; safeguarding an economic region covering 4.5 million square miles; and assisting people in distress or affected by natural and human-made disasters.[1]

The Coast Guard relies extensively on IT systems and services to carry out its missions. For example, it uses the Marine Information for Safety and Law Enforcement (MISLE) system to track and report data for nine of its 11 missions. Further emphasizing the importance of IT, the Coast Guard considers nearly every technology in the physical domain to be increasingly connected and dependent upon cyberspace.[2] Given this, it plans to spend $93 million in fiscal year 2022 to improve the reliability and

[1] 6 U.S.C. § 468.

[2] The Coast Guard defines cyberspace as the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded processors and controllers.

performance of its information systems and the underlying IT infrastructure.[3]

Federal policy highlights the need for federal agencies, including the Coast Guard, to enhance the management of IT resources.[4] In doing so, agencies should, among other things:

- focus IT resource planning to support agency missions;
- consider information security throughout the system development lifecycle; and
- rethink and restructure the way work is performed before investing in new information systems.

The *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* includes a provision for GAO to review several aspects of the Coast Guard's IT program.[5] Our specific objectives were to determine (1) the extent to which the Coast Guard has a process to ensure its IT infrastructure meets its current needs, including planning for network capacity; (2) the Coast Guard's cybersecurity risk management process for information technology and how, if at all, the process differs for operational technology; and (3) the extent to which the Coast Guard has incorporated federal requirements and guidance in its strategy for implementing cloud computing.

To address the first objective, we reviewed and summarized policies and procedures describing the Coast Guard's processes to ensure the adequacy of the service's (in this report, the service refers to the Coast Guard) IT infrastructure. For example, we reviewed operational assessment reports related to the Coast Guard's IT capabilities between

[3] IT infrastructure is the underlying framework of equipment, interconnected system, or subsystem of equipment that supports the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organization.

[4] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

[5] Elijah E. Cummings Coast Guard Authorization Act of 2020, Div. G of the William M. (Mac) Thornberry *National Defense Authorization Act for Fiscal Year 2021*, Pub. L. No. 116-283, § 8258, 134 Stat. 4633, 4677-4678 (Jan. 1, 2021).

October 2020 and September 2021 to identify any performance issues or user challenges.[6]

We also assessed the service's efforts to plan for adequate network capacity. To do this, we identified common practices for network capacity planning by collecting and reviewing publicly available federal agency capacity planning guidance, as well as industry guidance. The common practices we identified were:

1. compile a hardware, software, and configuration inventory;
2. identify the baseline network utilization and traffic growth predictions;
3. determine bandwidth allocation needs for variations and prioritize network traffic;
4. run simulations and what-if analyses; and
5. make refinements to the network and continually monitor the health of the network.

We then analyzed Coast Guard's actions to plan for network capacity and compared them to the common practices. We supplemented our analyses by interviewing relevant Coast Guard officials in the Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Program Management Office and C5I Service Center.

To address the second objective, we reviewed Coast Guard policies, procedures, and strategies to understand how the service is to apply risk management for IT and operational technology. We also compared the Coast Guard's risk management processes for IT and operational technology, determined whether the processes differed, and summarized both processes.

To determine if the service was following its cybersecurity risk management process for operational technology, we randomly selected a sample of eight systems listed as platform IT (one type of operational technology) in the Coast Guard's Enterprise Systems Inventory (ESI). For each of the selected systems, we analyzed available system security authorization documentation against Coast Guard process guides to

[6] Operational assessments are intended to identify user satisfaction and information regarding the effectiveness of capabilities deployed by Command, Control, Communications, Computers, Cyber, and Intelligence (C5I). The results of the assessments are documented in a report that is used to inform decision making and meet investment management reporting requirements.

determine how the Coast Guard applied its cybersecurity risk management process. We supplemented our analysis by interviewing relevant officials in the Coast Guard's Assistant Commandant for Command, Control, Communications, Computers, and IT (hereinafter referred to as C4&IT) and the Coast Guard's Cyber Command.

To address the third objective, we identified federal cloud computing requirements and guidance contained in the Office of Management and Budget's (OMB) *Federal Cloud Computing Strategy*, *Security Authorization of Information Systems in Cloud Computing Environments Memorandum*, and the President's Executive Order on *Improving the Nation's Cybersecurity*.[7] We summarized the requirements and guidance under the three pillars outlined in OMB's *Federal Cloud Computing Strategy*—security, procurement, and workforce.

We then compared the Coast Guard's cloud strategy and other cloud-related guidance to the summarized requirements. Where the Coast Guard's documentation lacked the required information, we evaluated the Department of Defense's (DOD) cloud-related strategies and guidance that the Coast Guard is required to follow.[8]

We supplemented our analysis with interviews of relevant Coast Guard officials in the C5I Program Management Office, the Office of Cyberspace Forces, and the Assistant Commandant for Acquisition. These interviews assisted in determining the status of ongoing cloud migrations and identifying future plans for cloud computing at the service. A more detailed description of our objectives, scope, and methodology can be found in appendix I.

We conducted this performance audit from April 2021 to July 2022 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

[7] Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019); OMB, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011); The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

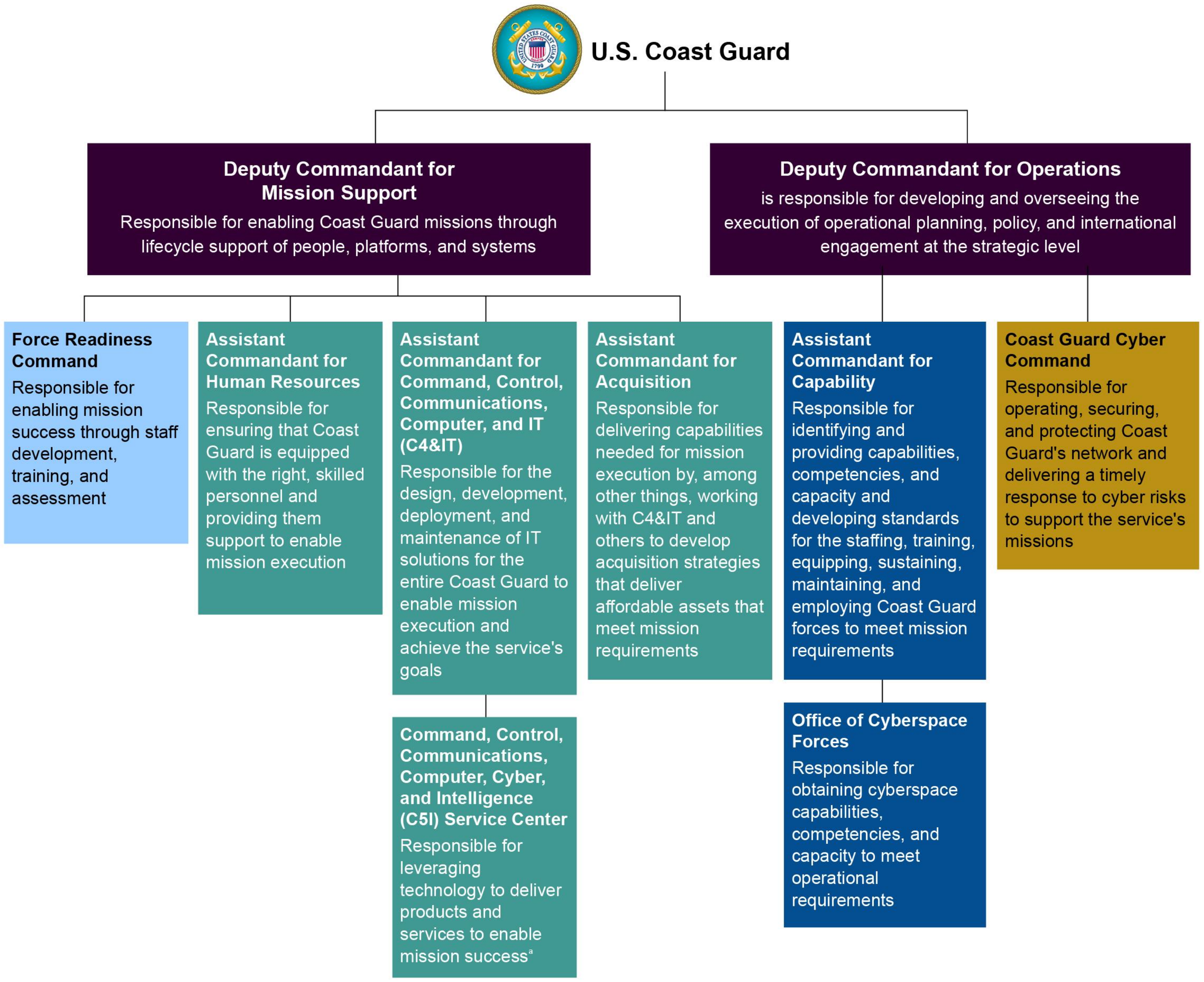
[8] In January 2017, the Secretaries of DOD and DHS signed an agreement regarding the Coast Guard's cooperation with DOD on cybersecurity and cyberspace operations. That agreement requires the Coast Guard to adhere to DOD cybersecurity requirements, standards, and policies for Coast Guard-operated systems and networks that are on the Department of Defense Information Network.

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.

Background

The management of federal IT programs spans a variety of activities, including the delivery of IT services, implementation of cybersecurity, maintenance of the cyberspace workforce, and oversight of IT acquisitions. Several Coast Guard units have responsibilities for managing the service's (in this report, the service refers to the Coast Guard) IT program. Figure 1 provides a description of the Coast Guard units with responsibilities for managing the service's IT program.

Figure 1: Coast Guard Units that Manage the Service’s Information Technology Program


U.S. Coast Guard
Deputy Commandant for Mission Support
Responsible for enabling Coast Guard missions through lifecycle support of people, platforms, and systems
Deputy Commandant for Operations
is responsible for developing and overseeing the execution of operational planning, policy, and international engagement at the strategic level
Force Readiness Command
Responsible for enabling mission success through staff development, training, and assessment
Assistant Commandant for Human Resources
Responsible for ensuring that Coast Guard is equipped with the right, skilled personnel and providing them support to enable mission execution
Assistant Commandant for Command, Control, Communications, Computer, and IT (C4&IT)
Responsible for the design, development, deployment, and maintenance of IT solutions for the entire Coast Guard to enable mission execution and achieve the service's goals
Assistant Commandant for Acquisition
Responsible for delivering capabilities needed for mission execution by, among other things, working with C4&IT and others to develop acquisition strategies that deliver affordable assets that meet mission requirements
Assistant Commandant for Capability
Responsible for identifying and providing capabilities, competencies, and capacity and developing standards for the staffing, training, equipping, sustaining, maintaining, and employing Coast Guard forces to meet mission requirements
Coast Guard Cyber Command
Responsible for operating, securing, and protecting Coast Guard's network and delivering a timely response to cyber risks to support the service's missions
Command, Control, Communications, Computer, Cyber, and Intelligence (C5I) Service Center
Responsible for leveraging technology to deliver products and services to enable mission success[a]
Office of Cyberspace Forces
Responsible for obtaining cyberspace capabilities, competencies, and capacity to meet operational requirements

Source: GAO analysis of Coast Guard documentation. | GAO-22-105092

Text of Figure 1: Coast Guard Units that Manage the Service’s Information Technology Program

1) U.S. Coast Guard

a) Deputy Commandant for Mission Support: Responsible for enabling Coast Guard missions through lifecycle support of people, platforms, and systems

  i) Force Readiness Command: Responsible for enabling mission success through staff development, training, and assessment

  ii) Assistant Commandant for Human Resources: Responsible for ensuring that Coast Guard is equipped with the right, skilled personnel and providing them support to enable mission execution

  iii) Assistant Commandant for Command, Control, Communications, Computer, and IT (C4&IT): Responsible for the design, development, deployment, and maintenance of IT solutions for the entire Coast Guard to enable mission execution and achieve the service's goals

    (1) Command, Control, Communications, Computer, Cyber, and Intelligence (C5I) Service Center: Responsible for leveraging technology to deliver products and services to enable mission success[a]

  iv) Assistant Commandant for Acquisition: Responsible for delivering capabilities needed for mission execution by, among other things, working with C4&IT and others to develop acquisition strategies that deliver affordable assets that meet mission requirements

b) Deputy Commandant for Operations: is responsible for developing and overseeing the execution of operational planning, policy, and international engagement at the strategic level

  i) Assistant Commandant for Capability: Responsible for identifying and providing capabilities, competencies, and capacity and developing standards for the staffing, training, equipping, sustaining, maintaining, and employing Coast Guard forces to meet mission requirements

    (1) Office of Cyberspace Forces: Responsible for obtaining cyberspace capabilities, competencies, and capacity to meet operational requirements

  ii) Coast Guard Cyber Command: Responsible for operating, securing, and protecting Coast Guard's network and delivering a timely response to cyber risks to support the service's missions

Note: In addition to the Coast Guard units identified in the figure, other programming offices may also provide support to the Coast Guard IT program.

[a]In addition to providing products and services to support C4&IT, the C5I Service Center also provides products and services to support offices in the Assistant Commandant for Capability, such as the Office for Cyberspace Forces and Coast Guard Cyber Command.

Source: GAO analysis of Coast Guard documentation. | GAO-22-105092

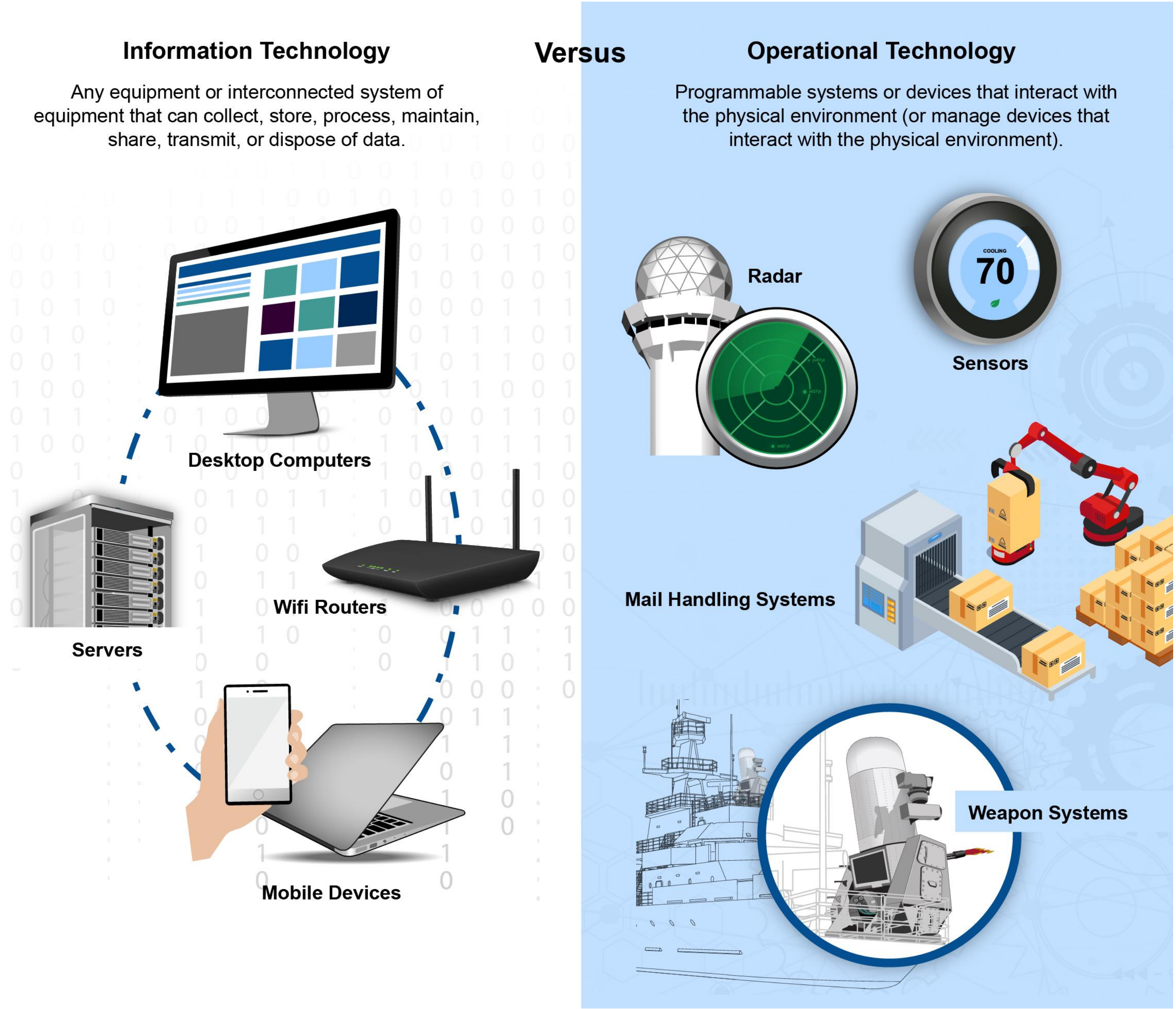
Operational Technology Helps Coast Guard to Meet Mission Needs

The Coast Guard's portion of the Department of Defense Information Network—the Enterprise Mission Platform—consists of both IT and operational technology. In addition to IT, the Coast Guard's service members rely on operational technology in almost every element of the service's cutter, aviation, and shore forces to conduct operations. The National Institute of Standards and Technology (NIST) defines operational technology as a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events.

Initially, operational technology systems were isolated, ran proprietary control protocols, and used specialized hardware and software. However, as operational technology are adopting IT solutions to promote connectivity and remote access capabilities, they have started to resemble IT systems.

Examples of common operational technology include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. It is important for agencies to protect operational technology from being compromised and accessed without authorization to avoid the disruption of critical devices or functions. Figure 2 depicts common types of IT and operational technology, and how they differ.

Figure 2: Common Types of Information Technology and Operational Technology


Information Technology
Any equipment or interconnected system of equipment that can collect, store, process, maintain, share, transmit, or dispose of data.
Versus
Operational Technology
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).
Desktop Computers
Servers
Wifi Routers
Mobile Devices
Radar
Sensors
COOLING
70
Mail Handling Systems
Weapon Systems

Source: GAO analysis of National Institute of Standards and Technology guidance and Coast Guard documentation; images: Vikivector/stock.adobe.com, kurtcan/stock.adobe.com, robu_s/stock.adobe.com, royyimzy/stock.adobe.com, Yevhenii/stock.adobe.com. | GAO-22-105092

According to officials in the Assistant Commandant for Command, Control, Communications, Computers, and IT (hereinafter referred to as C4&IT), Coast Guard operational technology consists of:

- **Platform IT.** Information technology, both hardware and software, that is physically part of, dedicated to, or essential in real time to performing the mission of either the platform (e.g., cutter or aircraft) or the special purpose system (e.g. gun weapon system, x-ray, or medical system). Examples of platform IT include weapon systems and training simulators.
- **Platform IT system (PIT system).** A system comprised of a collection of platform IT under the control of a single authority and security policy that may be structured by physical proximity or by function, independent of location. An example of a PIT system is a system that provides command and control for cutters through interfacing and integration with sensors and systems.
- **Industrial Control System (ICS).** IT systems used to control industrial processes and that consist of combinations of control components which act together to achieve an industrial objective. Examples of ICS include air traffic control and mail handling systems.
- **Supervisory Control and Data Acquisition (SCADA) system.** An ICS that is a computerized system capable of gathering and processing data and applying operational controls over long distances. SCADA systems are used in, for example, water distribution and wastewater collection systems, oil and natural gas pipelines, and electrical utility transmission and distribution systems.

Federal Policy and Guidance Established to Improve Agencies’ Management of IT

Federal policies and guidance highlight the importance of effectively managing and maintaining the cybersecurity of IT. For example, the Office of Management and Budget’s (OMB) policy on *Managing Information as a Strategic Resource* establishes requirements for the planning, budgeting, governance, acquisition, and management of federal information, IT resources, and supporting infrastructure and services, among other things.[9]

In addition, federal guidance also highlights the importance of protecting IT assets and the information they store and process. For example, the NIST *Risk Management Framework for Information Systems and*

[9] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016).

Organizations acknowledges the need for organizations to protect the confidentiality, integrity, and availability of information processed, stored, and transmitted on systems to support the success of missions and business functions.[10] The NIST risk management framework (RMF) provides guidelines for managing security and privacy risks and applying the framework to information systems and organizations.

Further, among other things, the May 2021 Executive Order on *Improving the Nation's Cybersecurity* sets forth policy for the prevention, detection, assessment, and remediation of cyber incidents.[11] The executive order requires that federal agencies protect and secure their computer systems, to include operational technology and systems that are cloud-based.[12]

In addition to emphasis on effective management and protection of IT assets, federal policies and guidance have stressed the importance of reducing acquisition and operating costs through the secure adoption of cloud computing. To that end, OMB's December 2011 memorandum on the *Security Authorization of Information Systems in Cloud Computing Environments* established the Federal Risk and Authorization Management Program (FedRAMP).[13] The FedRAMP program is intended to establish security requirements and guidelines that are to help secure cloud computing environments used by agencies. The memo describes key components of FedRAMP and its operational capabilities, and defines agency responsibilities for using FedRAMP.

Moreover, to provide additional guidance on implementing cloud solutions, OMB issued a *Federal Cloud Computing Strategy* in June

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

[11] The White House, *Improving the Nation's Cybersecurity*, Executive Order 14028 (Washington, D.C.: May 12, 2021).

[12] According to NIST, operational technology encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

[13] Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

2019.[14] The goal of this strategy is to provide actionable information and recommendations for agencies to accelerate adoption of cloud-based solutions. More specifically, the strategy emphasizes three pillars of successful cloud adoption—security, procurement, and workforce—and outlines requirements and guidance supporting each of the pillars.

Most recently, in January 2022, OMB released its memo on *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, which requires agencies to meet specific cybersecurity standards and objectives by the end of fiscal year 2024.[15] The memo highlighted the May 2021 Executive Order's government-wide effort for agencies to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

GAO Previously Reported Deficiencies in Coast Guard's IT Management

The Coast Guard has had longstanding issues with the management of its technology resources. We have previously reported deficiencies in the Coast Guard's implementation of its IT program. For example, in May 2022, we reported that Coast Guard needed to improve oversight of its non-major IT acquisition programs.[16] We found, for example, that the service's oversight of its non-major IT acquisition programs was hindered because programs are establishing, revising, and communicating cost and schedule goals (or baselines) inconsistently.

We made three recommendations to improve Coast Guard non-major IT acquisition oversight processes, including clearly communicating how

[14] Office of Management and Budget*, Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019) and *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011). The February 2011 strategy was intended to accelerate the government's use of cloud computing by requiring agencies to evaluate safe, secure cloud computing options before making any new investments.

[15] Office of Management and Budget, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Washington, D.C.: Jan. 26, 2022).

[16] GAO, *Coast Guard IT: Actions Needed to Improve Processes for Overseeing Non-Major Acquisition Programs,* GAO-22-104707 (Washington, D.C.: May 26, 2022). Non-major acquisition programs are programs with a total asset cost of less than $300 million.

programs should establish, revise, and communicate baseline information consistently. DHS concurred with all three recommendations.

In July 2020, we reported that the Coast Guard's MISLE system generally supported the service's operations, but that users reported numerous challenges that affected decision-making and accuracy of reporting.[17] These challenges included:

- **Data errors and inefficiencies due to the system's design.** For example, MISLE did not have system controls to prevent incomplete or duplicate entries—affecting service personnel's ability to conduct certain tasks.
- **Technology limitations affecting data use and efficiencies.** While MISLE allowed for exchanges of data between it and other Coast Guard databases, some users stated that the data exchanges were not fully integrated. Therefore, users had to reenter the same information into MISLE that already existed in other information systems.
- **Data collection issues.** For example, MISLE was unable to capture and collect various data that were needed to more accurately determine staffing needs and report on annual DHS-required performance measures, among other mission requirements.

We made four recommendations for the Coast Guard to improve data issues and system functionality in MISLE. The service agreed with all four recommendations and indicated that it planned to replace MISLE. In May 2022, Coast Guard officials stated that they believe replacing MISLE with a new enterprise-wide mission case management capability would address the recommendations we previously made. However, the Coast Guard had not yet acquired this capability and all four recommendations remained unaddressed at that time.

As another example, in January 2018, we reported that Coast Guard spent $59.9 million over nearly 7 years to implement a modernized electronic health records system. However, financial, technical, schedule, and personnel risks led to the service's decision to terminate the project without a useable system. Subsequently, the Coast Guard directed its clinics to revert to maintaining health records for its nearly 50,000 military

[17] GAO, *Coast Guard: Actions Needed to Ensure Investments in Key Data System Meet Mission and User Needs,* GAO-20-562 (Washington, D.C.: July 16, 2020).

personnel using a predominately paper process. As a result, its clinics faced numerous challenges related to incomplete records, tracking medications, and missing records, among many others.[18] We reported that the Coast Guard had begun taking steps to acquire a new electronic health records system, referred to as the Electronic Health Record Acquisition.

We made four recommendations to assist the Coast Guard in effectively acquiring and implementing an electronic health records solution to support the service's missions, to which the service agreed. In April 2018, the Coast Guard entered into an interagency agreement with the Defense Health Agency to procure the electronic health record system that the Department of Defense is implementing (Military Health System Genesis). As of February 2020, the service had addressed all four recommendations and planned to deploy the Military Health System Genesis by September 2022. The Coast Guard plans to deploy additional capabilities by June 2028.

Coast Guard Has Processes to Address Its IT Infrastructure but Lacks Network Capacity Planning

The Coast Guard implemented two processes intended to ensure that its IT infrastructure resources meet the service's mission needs. However, the service does not have a comprehensive process that included common practices for network capacity planning—a key process in IT infrastructure planning that involves assessing and determining the network resource needs required to effectively support an entity's mission.

[18] GAO, *Coast Guard Health Records: Timely Acquisition of New System Is Critical to Overcoming Challenges with Paper Process,* GAO-18-59 (Washington, D.C.: Jan. 24, 2018).

Coast Guard Has Two Processes Intended to Address IT Infrastructure Resources

OMB's guidance on *Managing Information as a Strategic Resource* states that agencies should implement processes to ensure that information resources, to include IT infrastructure, support agency missions and business needs.[19] The guidance also states that agencies should regularly assess the maintainability of its information resources and supporting infrastructure to actively determine when significant upgrades, replacements, and dispositions are required to effectively support agency missions.[20]

The Coast Guard has two processes intended to ensure the adequacy of its IT infrastructure—(1) the annual IT asset management and refresh and (2) C5I operational analysis processes:

Annual IT Management and Recapitalization Process

The *DHS IT Asset Management and Refresh Policy* requires the DHS Chief Information Officer (CIO) to regularly assess and refresh the current state of the department's IT infrastructure.[21] In supporting this responsibility, the Coast Guard CIO is to provide input into an annual DHS IT Infrastructure Assessment. This assessment involves implementing and maintaining policies, procedures, and controls to ensure proper management and recapitalization of IT infrastructure assets, and validating the annual refresh schedule that describes plans for recapitalizing those assets. As part of its IT management and recapitalization process, the Coast Guard CIO is responsible for working with the DHS CIO to maintain an annual implementation plan for the

[19] Office of Management and Budget, *Managing Information as a Strategic Resource*, Circular A-130 (Washington, D.C.: July 2016). As previously mentioned, IT infrastructure is the underlying framework of equipment, interconnected systems, or subsystems of equipment that supports the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an organization.

[20] Information resources are information and related resources, such as personnel, equipment, funds, and IT.

[21] According to the *DHS IT Asset Management and Recapitalization Process,* IT infrastructure includes desktops and laptops, servers, switches and routers, mobile devices, radios, printers, copiers, and scanners, imaging devices, sensors, and any related equipment, firmware, and operating software.

recapitalization and modernization of all IT infrastructure assets at the service. The plan is to include a timeline and spend plan for implementing these efforts.

The Coast Guard documented its most recent implementation plan in an IT Asset Refresh Implementation Report (refresh report) dated July 2020. The report states that the Coast Guard refreshes its IT hardware and software on about an 18-month schedule. According to the report, the service does this because many hardware and software manufacturers limit technical service support to the most current version and the two prior versions.[22]

Additionally, the refresh report states that the service uses a break/fix principle to refresh its IT. According to the report, this means that the service will refresh devices ahead of the planned 18-month refresh schedule in cases where operational impact is severe.[23] Conversely, if a device is fully functional, not exhibiting performance degradation, and within compliance of security standards, it may continue to operate the device beyond its planned 18-month refresh schedule. Coast Guard officials in the C5I Program Management Office stated that the service did not document a refresh report in 2021 due to limited staffing resources, and as of July 2022 had set a deadline of September 30, 2022, for the next report.

C5I Operational Analysis Process

The C5I Operational Analysis process is intended to determine whether the service's operational capabilities, programs, and systems are meeting mission requirements and addressing user needs. The Coast Guard Office of C5I Capabilities is responsible for performing the operational analysis by:

1. reviewing existing documentation describing the operational requirements and status of the capability;

[22] For example, if a software provider releases a new version about every 6 to 12 months and ends service support about 18 months later, renewing the versions every 2 years should assure that the Coast Guard has a supported version of software.

[23] According to the refresh report, cases of severe operational impact include situations where a device has become unreliable, damaged, or incompatible with a new software upgrade.

2. planning and executing site visits at Coast Guard offices and districts to gather operator feedback on the capabilities;
3. obtaining documentation of user satisfaction and key findings regarding the effectiveness of C5I capabilities deployed at the Coast Guard; and
4. coordinating with C5I stakeholders to make decisions based on the findings in the operational analysis.

The Coast Guard is to document its findings from the operational analysis in annual C5I State of the Capability Reports. These reports include recommendations intended to address any identified capability gaps, which are to be reviewed, validated, and managed through the *C5I Requirements Intake Process*. During the validation phase of the requirements intake process, the C5I Sponsor's Representative is to conduct an analysis to better understand the appropriate solutions to address an identified gap. The sponsor's representative is then to document the operational requirements needed for the proposed solution in a Requirements Use Case Catalog, and share the catalog with appropriate stakeholders.[24] If approved, the proposed solution is to be prioritized and eventually funded and executed.

In fiscal year 2021, the Coast Guard documented its results from operational analyses performed on 33 capabilities, to include the service's network and IT infrastructure. The Coast Guard's May 2021 State of the Capability Report for the Network and IT Infrastructure program identified issues with the adequacy of the service's remote access tools and cutter connectivity. As listed in the report, the C5I Sponsor's Representative for the network and IT infrastructure capability recommended a cutter connectivity capability that enables users to execute the service's mission with no degradation, among other things. The sponsor's representative prepared a Requirements and Use Case Catalog for the cutter connectivity capability, which was reviewed by relevant stakeholders. In December 2021, officials in the C5I Service Center stated that the service was preparing a solicitation for the capability, and hoped to deploy the enhanced cutter connectivity capability within the next 2-3 years.

[24] The *Coast Guard Operational Requirements Generation Manual* provides guidance on how the service is to identify and document operational requirements that are intended to meet the service's specific needs. The process of identifying, reviewing, and validating operational requirements is to ensure traceability between strategic objectives and capability investments.

Coast Guard Lacks a Comprehensive Process for Network Capacity Planning

Network capacity planning is a key process in IT infrastructure planning that is intended to determine the network resources required to effectively deliver on mission execution. Discrepancies in network capacity and demand for bandwidth result in inefficiencies associated with either underutilized resources or unmet performance expectations. We identified the following common practices for network capacity planning, which are intended to be completed in the specified order: [25]

1. **Compile an inventory of hardware, software, and configurations.** To start the network capacity planning process, organizations should compile an accurate inventory of all current hardware, software, and configurations on the network. Doing so allows organizations to fully understand what is on their network, thereby informing quick decision making to address capacity issues that may arise.
2. **Identify the baseline network utilization and traffic growth predictions.** The second step in network capacity planning is to determine the amount of incoming and outgoing traffic across the core network—a process known as baselining network utilization. In addition, identify traffic growth predictions to accommodate changes, such as adding additional staff to the network or deploying new software. Tracking and forecasting traffic utilization of system resources allows network administrators to plan and complete network upgrades before problems with capacity develop and cause service disruptions and network downtime.
3. **Determine bandwidth allocation needs for variations and prioritize network traffic.** After understanding network utilization and predicting potential network traffic growth, the next step focuses on determining the appropriate amount of bandwidth needed to accommodate the incoming and outgoing network traffic determined in the prior step. In this process, organizations should consider variations in traffic demand, such as sudden increases in bandwidth usage that may cause temporary congestion and service disruptions on the network. Additionally, organizations should prioritize different categories of network traffic, also known as implementing quality of

[25] We identified five common capacity planning practices from available industry white papers from Cisco and SolarWinds; federal capacity planning guidance from the Internal Revenue Service and Centers for Disease Control and Prevention; and articles on network capacity planning from Comparitech and Computerworld, among others.

service. For example, organizations can prioritize latency-sensitive data (e.g., voice data) over non-latency-sensitive data (e.g., emails) to ensure reliable communications.

4. **Run simulations and perform analyses of network usage.** Using the information from each of the steps above, the next step is to conduct simulations of network usage to show the forecasted traffic at different points on the network. The results of the simulation can be used to identify bottlenecks of bandwidth or areas where increased capacity is needed. Analyses of the forecasted traffic and what is currently provisioned on the network assist with determining the bandwidth required to achieve desired performance, and help administrators to better understand the effects of sudden increases in bandwidth consumption on their network. Further, network analyses can help to predict the results of a planned change on network utilization and resource issues, increasing the chance of success in deploying new technology.
5. **Make refinements to the network and continually monitor the health of the infrastructure.** The final step is to address any deficiencies identified while completing the prior steps by, for example, adding additional resources or making changes to the network. Additionally, organizations should continually monitor the health of their infrastructure to ensure that it is meeting changing demands, such as new users or systems, and fulfilling mission needs.

The Coast Guard partially implemented four of the common practices that we identified for network capacity planning and did not implement one. Table 1 provides a description of the Coast Guard's actions related to each of the network capacity planning common practices.

Table 1: Assessment of Coast Guard's Actions to Address Common Practices for Network Capacity Planning

Common practices for network capacity planning	Implementation status	Coast Guard actions
Compile an inventory of hardware, software, and configurations	Partially addressed	The Coast Guard has taken steps to compile hardware, software, and configuration inventories. However, Coast Guard officials in the Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Service Center stated that these inventories are maintained using multiple tracking tools and that they are incomplete and inaccurate.
Identify the baseline network utilization and traffic growth predictions	Partially addressed	The Coast Guard uses one tool to obtain information regarding network traffic volume and usage, and another tool to obtain information on network traffic volume and circuit utilization, or bandwidth consumption. However, Coast Guard officials in the C5I Program Management Office stated that the service was not using the information to establish baseline network utilization and identify traffic growth predictions.

Common practices for network capacity planning	Implementation status	Coast Guard actions
Determine bandwidth allocation needs for variations and prioritize network traffic	Partially addressed	As a general practice, Coast Guard's network engineers look for consistent bandwidth consumption of 70 percent or above before recommending capacity increases. However, delaying decisions to increase capacity until the network reaches bandwidth consumption of 70 percent or higher may not be sufficient in mitigating any disruptions caused by network traffic congestion during times when there are a high number of requests being made over the network. Additionally, the Coast Guard does not have the capability to prioritize traffic on its network. According to officials in the C5I Program Management Office, the service anticipates finalizing functional requirements needed for such a capability by the end of fiscal year 2022 and plans to initiate a project to implement the capability in fiscal year 2023.
Run simulations and perform analyses of network usage	Not addressed	The Coast Guard does not have a network modeling tool for running simulations and performing analyses. According to officials in the C5I Program Management Office, the Coast Guard identified this as an issue approximately five years ago as more of its systems were using limited bandwidth.
Make refinements to the network and continually monitor the health of the infrastructure	Partially addressed	The Coast Guard uses various tools to assist them in the decision-making process to modify network capacity when a request for increased capacity is received. Additionally, the Coast Guard has processes intended to facilitate annual monitoring of the health of the service's infrastructure. However, the Chief of Infrastructure Services stated that their processes to ensure adequate IT resources are reactive and not proactive—taking action when infrastructure issues arise.

Legend:

● = Addressed: The Coast Guard demonstrated that it had fully implemented the practice.

◑ = Partially addressed: The Coast Guard demonstrated that it implemented some, but not all of the practice.

○ = Not addressed: The Coast Guard could not demonstrate that it had implemented the practice.

Source: GAO analysis of U.S Coast Guard documentation and industry publications. | GAO-22-105092

The Coast Guard has not fully implemented network capacity planning due in part to its lack of documented policies and procedures for it. *Standards for Internal Control in the Federal Government* state that organizations should establish policies and procedures to document their activities to achieve objectives.[26] Instead, officials in C4&IT stated that the Coast Guard uses an undocumented, ad hoc process to manage the capacity on its network. According to officials in the C5I Program Management Office, the ad hoc process leverages their engineers' prior experience and customer reports to determine when and where additional capacity is needed.

The lack of comprehensive policies and procedures for capacity planning hinders the service's ability to proactively, rather than reactively, address IT infrastructure issues in a timely manner. Without fully implementing

[26] GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

capacity planning practices, the Coast Guard faces substantial risks in resulting inefficiencies and disruptions in network availability to users.

Coast Guard's IT Cybersecurity Risk Management Process Differs for Operational Technology and Has Been Inconsistently Applied

The Coast Guard is to follow the DOD's Risk Management Framework (RMF), which establishes two different cybersecurity risk management processes for identifying and applying cybersecurity controls to IT and certain operational technology resources. However, the service did not consistently apply the framework to its operational technology. In addition, it lacks a cybersecurity risk management process for two types of operational technology—industrial control systems and supervisory control and data acquisition systems.

Coast Guard Established a Cybersecurity Risk Management Process for IT and Certain Operational Technology

The NIST Risk Management Framework (RMF) states that agencies should apply a cybersecurity risk management process to all systems, including operational technology, to comprehensively manage risks to those systems.[27] To address this requirement, Coast Guard established two risk management processes for cybersecurity. Specifically, as of January 2017, the Coast Guard is required by an agreement between DOD and DHS to follow the *Risk Management Framework for DOD IT*, or the DOD RMF. The DOD RMF generally aligns with the NIST framework. The *U.S. Coast Guard Cybersecurity Manual* describes the service's two cybersecurity risk management processes for applying the DOD RMF to

[27] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Special Publication 800-37, Revision 2 (Gaithersburg, MD: December 2018).

identify, implement, and assess cybersecurity controls for (1) IT and PIT systems, and (2) operational technology.

Cybersecurity Risk Management Process for IT and PIT Systems

In accordance with the DOD RMF, the Coast Guard's cybersecurity risk management process for IT and PIT systems consists of six steps, as described below.[28]

1. **Categorize.** To guide and inform risk management processes, systems are categorized in accordance with NIST's *Federal Information Processing Standards Publication 199* (FIPS 199).[29] FIPS 199 uses a security breach's impact on the compromise or loss of confidentiality, integrity, and availability of organizational assets to categorize systems.[30]
2. **Select.** Identify security controls based on the system categorization performed in step one by using NIST and the Committee on National Security System's (CNSS) guidance on security control selection, as applicable.[31] Document the security controls in a system security plan (SSP).
3. **Implement.** Deploy the identified security controls within the system, and document the description and implementation status of each control in the SSP.
4. **Assess.** Test the security controls to determine whether the controls are effective, implemented correctly, and meet the system's security requirements. Document the results of the control testing in the

[28] Although the Coast Guard considers PIT systems to be operational technology, the *U.S. Coast Guard Cybersecurity Manual* requires that PIT systems follow the same RMF process as IT systems.

[29] NIST, *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

[30] FIPS 199 defines impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals.

[31] The *U.S. Coast Guard Cybersecurity Manual* directs the service to select controls based on guidance in the NIST *Security and Privacy Controls for Federal Information Systems and Organizations,* Special Publication 800-53, Revision 4. The manual also directs the service to use the CNSS *Security Categorization and Control Selection for National Security Systems,* Instruction No. 1253 for selecting controls for national security systems.

security assessment report. Record all identified vulnerabilities in a plan of action and milestones (POA&M) report. IT and PIT systems are to be reassessed every three years.

5. **Authorize.** After documenting the remedial actions in a POA&M report, the authorizing official is to review all of the system security-related documentation described above to make a determination to either grant or deny an authorization to operate.[32]
6. **Monitor.** Develop and document a system-level strategy for continuous monitoring of security control effectiveness, and monitor any proposed or actual changes that may negatively affect the security posture of the system and its operating environment for the duration of the authorization to operate.[33]

In January 2022, subsequent to the start of this review, the service issued its Ongoing Authorization Policy to facilitate continuous monitoring of system risks once authorization is granted. The policy provides guidance for implementing continuous monitoring by transitioning from the three-year reassessment requirement to a continual process for authorizing information systems and PIT systems. In doing so, the policy outlines responsibilities for various stakeholders to implement continuous monitoring.

Cybersecurity Risk Management Process for Operational Technology

In accordance with the DOD RMF, the Coast Guard is to follow a shortened cybersecurity risk management process for platform IT—one type of operational technology. Specifically, the Coast Guard's process for platform IT follows steps one through four of the full six-step RMF: (1) Categorize, (2) Select, (3) Implement, and (4) Assess.

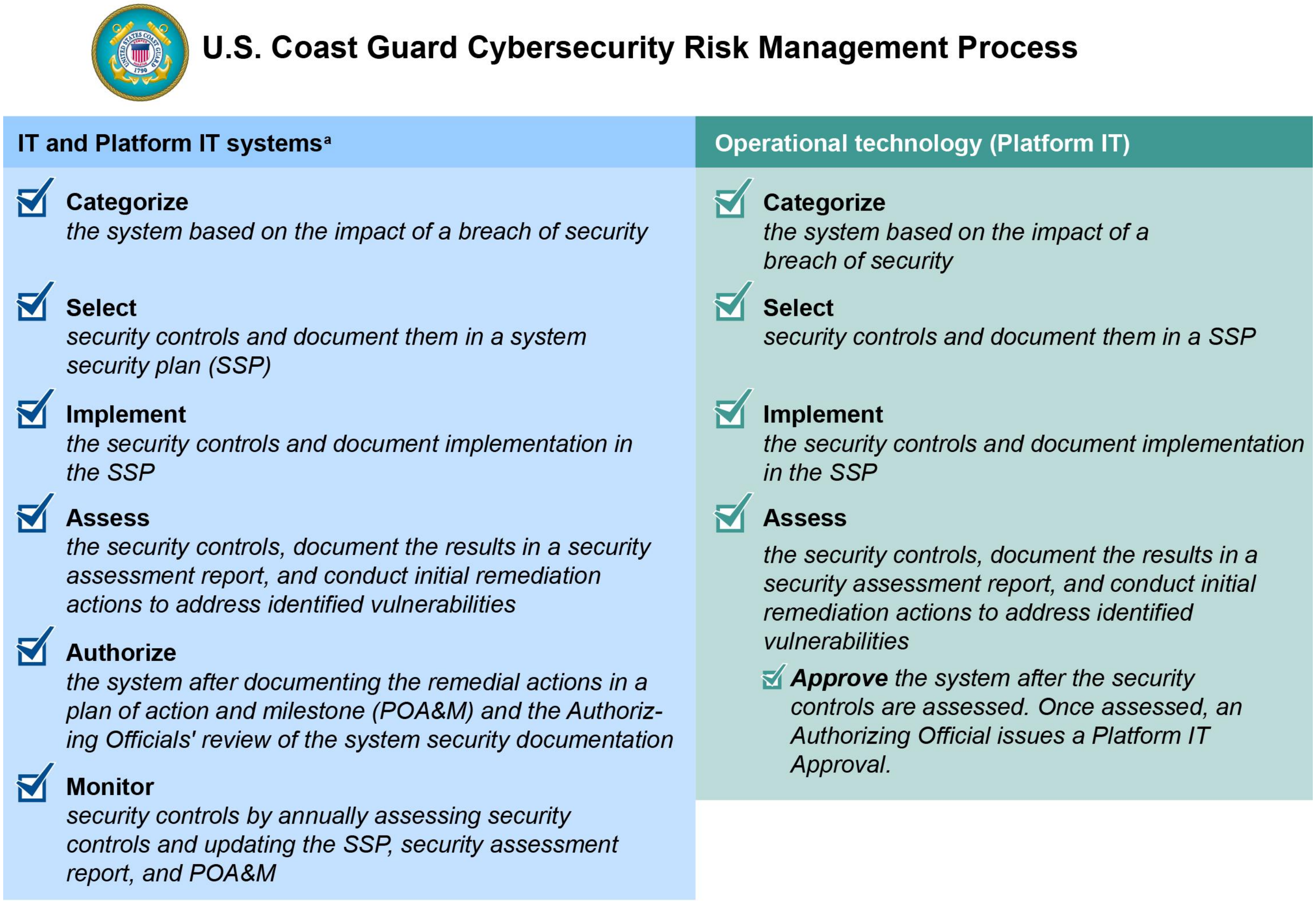
According to the Coast Guard's cybersecurity risk management process, platform IT does not go through the *Authorize* or *Monitor* steps—the last two steps of the full DOD RMF. Instead, the authorizing official grants a

[32] An authorization to operate is the official management decision to operate a system and to explicitly accept the risk to organizational operations. All Coast Guard IT and PIT systems must have a valid authorization to operate prior to operational use.

[33] According to NIST, continuous monitoring is the process of maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Ongoing awareness means that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

platform IT approval once the selected security controls are assessed at step four and the necessary security requirements have been implemented. The platform IT approval documents the authorizing official’s approval for the platform IT to be operational. Unlike the authorization to operate process required for IT and PIT systems, the platform IT approval does not require reassessment every three years. Upon obtaining the approval, the approval is maintained for the life of the platform IT. Reassessment is only required if there is a configuration change. Figure 3 depicts the two different risk management approaches that Coast Guard uses for IT, PIT systems, and platform IT.

Figure 3: Coast Guard Cybersecurity Risk Management Process for Information Technology and Operational Technology



U.S. Coast Guard Cybersecurity Risk Management Process

IT and Platform IT systems[a]

☑ **Categorize** *the system based on the impact of a breach of security*

☑ **Select** *security controls and document them in a system security plan (SSP)*

☑ **Implement** *the security controls and document implementation in the SSP*

☑ **Assess** *the security controls, document the results in a security assessment report, and conduct initial remediation actions to address identified vulnerabilities*

☑ **Authorize** *the system after documenting the remedial actions in a plan of action and milestone (POA&M) and the Authorizing Officials' review of the system security documentation*

☑ **Monitor** *security controls by annually assessing security controls and updating the SSP, security assessment report, and POA&M*

Operational technology (Platform IT)

☑ **Categorize** *the system based on the impact of a breach of security*

☑ **Select** *security controls and document them in a SSP*

☑ **Implement** *the security controls and document implementation in the SSP*

☑ **Assess** *the security controls, document the results in a security assessment report, and conduct initial remediation actions to address identified vulnerabilities*

☑ ***Approve** the system after the security controls are assessed. Once assessed, an Authorizing Official issues a Platform IT Approval.*

Source: GAO analysis of the U.S. Coast Guard Cybersecurity Manual. | GAO-22-105092

Text of Figure 3: Coast Guard Cybersecurity Risk Management Process for Information Technology and Operational Technology

IT and Platform IT systems/a/

- Categorize the system based on the impact of a breach of security
- Select security controls and document them in a system security plan (SSP)
- Implement the security controls and document implementation in the SSP

- Assess the security controls, document the results in a security assessment report, and conduct initial remediation actions to address identified vulnerabilities
- Authorize the system after documenting the remedial actions in a plan of action and milestone (POA&M) and the Authorizing Officials' review of the system security documentation
- Monitor security controls by annually assessing security controls and updating the SSP, security assessment report, and POA&M

Operational technology (Platform IT)

- Categorize the system based on the impact of a breach of security
- Select security controls and document them in a SSP
- Implement the security controls and document implementation in the SSP
- Assess the security controls, document the results in a security assessment report, and conduct initial remediation actions to address identified vulnerabilities
    - Approve the system after the security controls are assessed. Once assessed, an Authorizing Official issues a Platform IT Approval.

[a] Although the Coast Guard considers platform IT systems to be operational technology, the U.S. Coast Guard Cybersecurity Manual requires that these systems follow all six steps of the *Risk Management Framework for Department of Defense IT*.

Source: GAO analysis of the U.S. Coast Guard Cybersecurity Manual. | GAO-22-105092

Coast Guard Did Not Consistently Apply Its Cybersecurity Risk Management Process for Operational Technology

The Coast Guard did not consistently apply its cybersecurity risk management process for operational technology. Specifically, for the eight systems identified as platform IT that we selected:

- The Coast Guard applied its process for three systems that we selected.
- The Coast Guard initiated, but had not completed, the cybersecurity risk management process for two systems that are noted in the service’s systems inventory as in the operations and maintenance phase of the systems engineering life cycle.

- For one Coast Guard-owned system that is operated by the U.S. Navy, the service could not demonstrate that it had obtained and approved a complete security authorization package from the Navy, as required by the Coast Guard's cybersecurity risk management process.[34]
- For two other systems, the Coast Guard could not demonstrate that it had applied the cybersecurity risk management process to those systems. For one of these systems, the service stated that it inaccurately entered the system into the systems inventory because it did not consider them as either IT or operational technology. For the other system, officials in the Assistant Commandant for Capability stated that the service's Aviation Logistics Center was working on developing the required security authorization documentation.

An Incomplete and Inaccurate Inventory Contributed to Inconsistent Application of the Cybersecurity Risk Management Process

The Coast Guard did not consistently implement its cybersecurity risk management process for platform IT, in part, because the inventory system that the Coast Guard uses to track IT and operational technology—the Enterprise System Inventory (ESI)—contained inaccurate and incomplete information. For example, as described above, officials stated that it had entered one of the systems we selected into ESI in error, and that it should have listed two other systems in the inventory as IT, instead of platform IT. In addition, the Coast Guard's ESI does not include all of the service's operational technology. Specifically, the Coast Guard does not track ICS and SCADA systems. According to officials, these systems were not inventoried and tracked within ESI because of resource constraints.

[34] The *U.S. Coast Guard Cybersecurity Manual* allows the service to enter mutual agreements with other organizations to accept each other's security assessments in order to reuse information system resources. This process is known as reciprocity. The manual requires a deploying organization (in this case Navy) to provide the complete security authorization package for shared systems to the receiving organization (in this case Coast Guard). Additionally, the receiving organization is required to update the authorization to operate to include any additional or modified security controls associated with hosting the deployed system.

Change in Policy Resulted in Missed Application of the Cybersecurity Risk Management Process for Operational Technology

Another reason the Coast Guard did not consistently implement its cybersecurity risk management process for platform IT is that the policy for assessing operational technology has changed over time. According to officials in C4&IT, prior to the January 2017 requirement for the Coast Guard to follow the DOD RMF, the service had not formally assessed platform IT for cybersecurity controls. Instead, as required by the policy in place at that time, the service implemented tailored security controls on these systems, and only reassessed them when the systems underwent a major configuration change. However, the Coast Guard could not demonstrate that it had implemented or assessed security controls at any time for at least four platform IT we selected. According to officials in C4&IT, as of February 2022, the service was preparing to apply its cybersecurity risk management process to at least two of the platform IT we selected. However, at that time, the Coast Guard did not have a plan or schedule for ensuring all platform IT at the service meet DOD RMF requirements.

Without a comprehensive inventory of all systems, including all operational technology, the service cannot ensure that it is applying adequate cybersecurity measures to all systems and devices on its network. Additionally, without consistently applying a cybersecurity risk management process to platform IT, the Coast Guard risks unauthorized access to those systems or devices, potentially leading to system disruptions and loss of data.

Coast Guard Does Not Have a Cybersecurity Risk Management Process for ICS and SCADA Systems

According to the NIST RMF and other guidance, agencies should apply a cybersecurity risk management process to all systems. To comprehensively manage risks, this is to include ICS and SCADA systems.[35]

[35] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2 (Gaithersburg, Md.: Dec. 2018) and *Guide to Industrial Control Systems (ICS) Security*, NIST Special Publication 800-82, Revision 2, Gaithersburg, MD: May 2015).

Although the *U.S. Coast Guard Cybersecurity Manual* describes the service's cybersecurity risk management process for IT and some operational technology (platform IT and PIT systems), the Coast Guard lacks a cybersecurity risk management process for ICS and SCADA systems. In April 2022, Coast Guard officials in C4&IT stated that the risk management process outlined in the cybersecurity manual is also applicable to ICS and SCADA systems.

However, the manual does not explicitly describe how the service is to apply the process for those systems. Without a cybersecurity risk management process for ICS and SCADA systems, the Coast Guard cannot ensure that it is effectively managing risks to those systems.

Coast Guard Incorporated Most Federal Cloud Requirements into Its Strategy and Policies

The *U.S. Coast Guard Cloud Strategy for 2021 - 2026* and other relevant documentation included most of the requirements and guidance related to the three pillars of federal cloud computing—security, procurement, and workforce. Specifically, the documentation:

- fully addressed nine of the ten security-related requirements, and did not address the remaining requirement;
- included all eight procurement-related cloud computing requirements; and
- fully included two, and partially included two other workforce-related requirements.

Coast Guard Policies Include Most Federal Cloud Computing Requirements

OMB's December 2011 memo on *Security Authorization of Information Systems in Cloud Computing Environments* sets policy for federal agencies to protect information in the cloud through adoption of the Federal Risk and Authorization Management Program (FedRAMP).[36] Subsequent to releasing the December 2011 memo, in June 2019, OMB

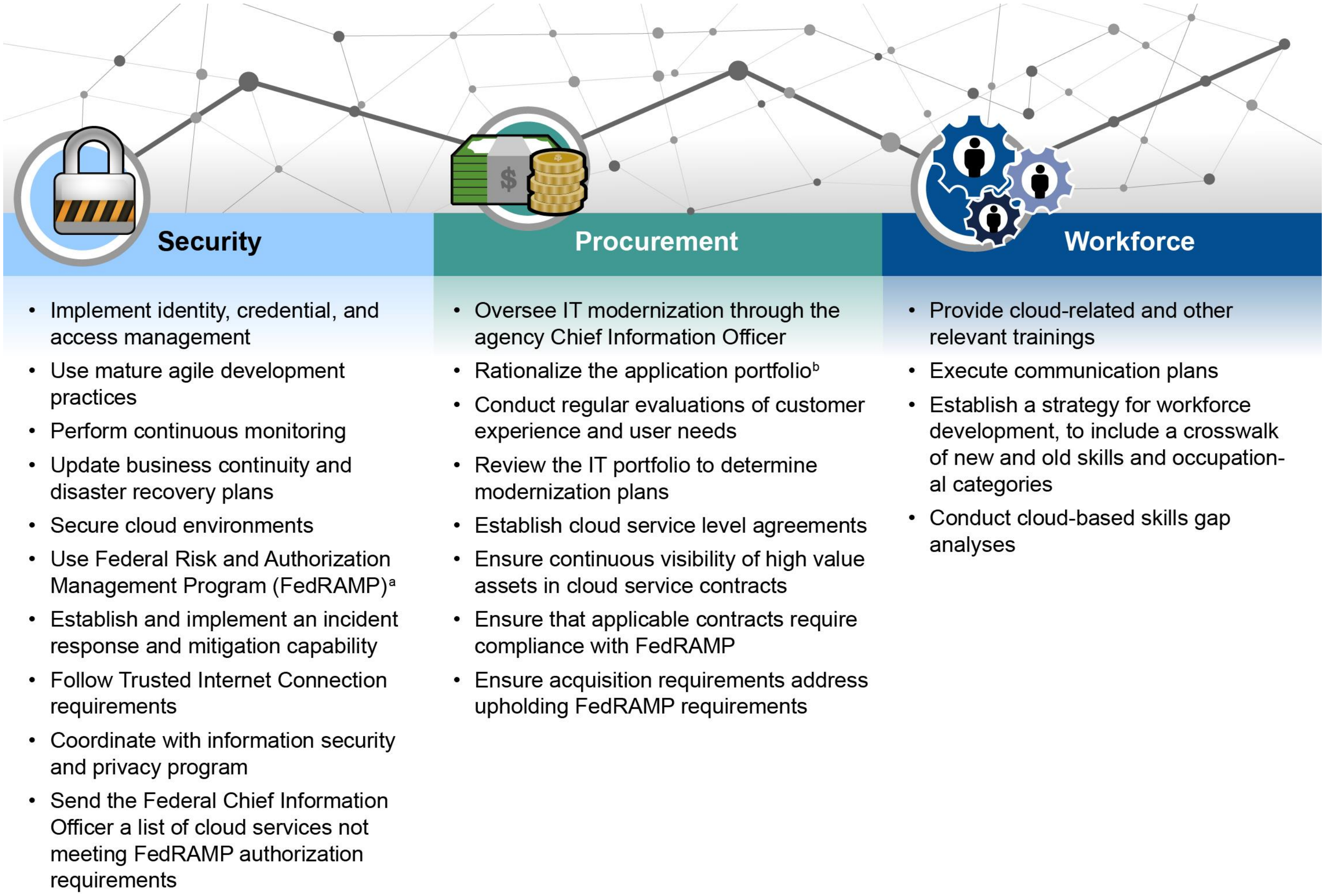
[36] Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

issued the *Federal Cloud Computing Strategy* that includes requirements and guidance for federal agencies to implement cloud computing.[37] The strategy outlines three key pillars intended for successful cloud adoption—security, procurement, and workforce.

As shown in figure 4, the requirements and guidance described in the aforementioned federal documents can be categorized into the three key pillars outlined in OMB's *Federal Cloud Computing Strategy*. Appendix II provides a detailed description of the requirements and guidance in each of the three areas.

[37] Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019).

Figure 4: Federal Requirements and Guidance for Cloud Computing



Security

- Implement identity, credential, and access management
- Use mature agile development practices
- Perform continuous monitoring
- Update business continuity and disaster recovery plans
- Secure cloud environments
- Use Federal Risk and Authorization Management Program (FedRAMP)[a]
- Establish and implement an incident response and mitigation capability
- Follow Trusted Internet Connection requirements
- Coordinate with information security and privacy program
- Send the Federal Chief Information Officer a list of cloud services not meeting FedRAMP authorization requirements

Procurement

- Oversee IT modernization through the agency Chief Information Officer
- Rationalize the application portfolio[b]
- Conduct regular evaluations of customer experience and user needs
- Review the IT portfolio to determine modernization plans
- Establish cloud service level agreements
- Ensure continuous visibility of high value assets in cloud service contracts
- Ensure that applicable contracts require compliance with FedRAMP
- Ensure acquisition requirements address upholding FedRAMP requirements

Workforce

- Provide cloud-related and other relevant trainings
- Execute communication plans
- Establish a strategy for workforce development, to include a crosswalk of new and old skills and occupational categories
- Conduct cloud-based skills gap analyses

Source: GAO analysis of the Office and Management and Budget's Federal Cloud Computing Strategy issued in June 2019 and Security Authorization of Information Systems in Cloud Computing Environments. | GAO-22-105092

Text of Figure 4: Federal Requirements and Guidance for Cloud Computing

Security

- Implement identity, credential, and access management
- Use mature agile development practices
- Perform continuous monitoring
- Update business continuity and disaster recovery plans
- Secure cloud environments

- Use Federal Risk and Authorization Management Program (FedRAMP)[a]
- Establish and implement an incident response and mitigation capability
- Follow Trusted Internet Connection requirements
- Coordinate with information security and privacy program
- Send the Federal Chief Information Officer a list of cloud services not meeting FedRAMP authorization requirements

Procurement

- Oversee IT modernization through the agency Chief Information Officer
- Rationalize the application portfolio[b]
- Conduct regular evaluations of customer experience and user needs
- Review the IT portfolio to determine modernization plans
- Establish cloud service level agreements
- Ensure continuous visibility of high value assets in cloud service contracts
- Ensure that applicable contracts require compliance with FedRAMP
- Ensure acquisition requirements address upholding FedRAMP requirements

Workforce

- Provide cloud-related and other relevant trainings
- Execute communication plans
- Establish a strategy for workforce development, to include a crosswalk of new and old skills and occupational categories
- Conduct cloud-based skills gap analyses

[a] The Office of Management and Budget (OMB) established FedRAMP in 2011 to provide standardization for selecting and authorizing cloud services.

[b] According to the Chief Information Officers Council and Cloud & Infrastructure Community of Practice, application rationalization is the effort to strategically identify business applications across an organization to determine which should be kept, replaced, retired, or consolidated.

Source: GAO analysis of the Office and Management and Budget's Federal Cloud Computing Strategy issued in June 2019 and Security Authorization of Information Systems in Cloud Computing Environments. | GAO-22-105092

The Coast Guard issued the *U.S. Coast Guard Cloud Strategy for 2021 - 2026* in March 2021. The strategy outlines several strategic objectives for cloud computing and describes the service's priorities for IT modernization efforts over the next five years.[38] The Coast Guard's cloud strategy and other related documentation included most of the federal requirements and guidance we identified. As described below, the strategy and other documentation either fully or partially addressed most of the requirements and guidance related to each of the key pillars for cloud adoption—security, procurement, and workforce.

Coast Guard Incorporated Most of the Security-Related Requirements and Guidance

The 2019 *Federal Cloud Computing Strategy* identifies security as one of the three pillars of successful cloud adoption. According to the strategy, the security pillar emphasizes the need to modernize security policies in an effort to focus on risk based decision-making, automations, and data protection.

The *U.S. Coast Guard Cloud Strategy for 2021 - 2026* and other supporting documentation included most of the security-related requirements we identified. Specifically, the documentation fully addressed nine of the ten security-related requirements and did not address another requirement. Table 2 below describes the extent to which the service incorporated security-related federal cloud computing requirements and guidance in its documentation.

Table 2: Extent Coast Guard Incorporated Security-Related Federal Cloud Computing Requirements and Guidance in the Service's Cloud Strategy and Supporting Documentation

Security-related federal requirements & guidance	Status	GAO assessment
Implement identity, credential, and access management	fully addressed	The *Department of Defense (DOD) Identity, Credential, and Access Management (ICAM)* Strategy outlines activities for deploying ICAM capabilities for information systems, including cloud based systems. The strategy highlights the need to deploy ICAM capabilities to support a rapid and secure adoption of cloud services.

[38] As of April 2022, the Coast Guard migrated to four cloud services and was in the process of transitioning to three additional cloud services. Appendix III provides a description and status of each of the Coast Guard's completed and planned migrations.

Security-related federal requirements & guidance	Status	GAO assessment
Use mature agile development practices, to include development, security, and operations (DevSecOps)[a]	fully addressed	The *DOD Enterprise DevSecOps Reference Design* requires the service to implement an agile software development methodology that incorporates security throughout the process—commonly referred to as DevSecOps. The *U.S. Coast Guard Cloud Strategy for 2021-2026* describes the service's plans to consider DevSecOps concepts to provide capabilities that leverage cloud capacity, speed, and analytical insight, while also considering security throughout the lifecycle of data and technology. According to the plan, doing so will ensure the security of large amounts of data and safeguard its critical assets.
Perform continuous monitoring	fully addressed	The *DOD Cloud Computing Security Requirements Guide* requires an ongoing assessment and authorization capability, including continuous monitoring, for cloud service offerings. The guide includes continuous monitoring activities such as regularly conducting vulnerability scans, annually assessing controls, and notifying the service of significant changes to the cloud service, among others. Additionally, the *DOD Cloud Acquisition Guidebook* includes the required contract language for the cloud service provider to provide the service with continuous monitoring reports.
Update business continuity and disaster recovery plans	fully addressed	The *DOD Cloud Computing Acquisition Guidebook* includes contract language for the cloud service provider. The contract language outlines responsibilities for cloud service providers in cases of an interruption of cloud services. Additionally, the guide provides examples of service level agreement performance measures that include responsibilities for the cloud service provider to provide continuity of operations and disaster recovery planning and testing. Further, the service is to follow the *DOD Cloud Computing Security Requirement Guide*, which includes continuity of operations and disaster recovery requirements for the cloud service provider. For example, the guide notes that it is a best practice for the cloud service provider to plan for continuity of operations and disaster recovery, and to implement the infrastructure to support it.
Secure cloud environments	fully addressed	The *DOD Cloud Computing Security Requirements Guide* describes an approach for using a multi-layer defense strategy, or the defense-in-depth concept, when protecting its networks and information. This approach includes hardening host operating systems and applications, implementing strong access controls, monitoring system events, and protecting the service's networks.
Use the Federal Risk and Authorization Management Program (FedRAMP)	fully addressed	The *DOD Cloud Computing Security Requirements Guide* requires the service to implement FedRAMP's moderate- and high-security baseline requirements, as appropriate, along with additional requirements to meet and assure the service's critical mission needs for cloud services. A DOD memo providing guidance on the acquisition and use of commercial cloud computing services states that FedRAMP serves as the minimum security baseline for all DOD cloud services, including those at Coast Guard. Additionally, the guide requires the use of the DOD risk management framework to grant an authorization to operate cloud services.[b] According to the *DOD Cloud Computing Security Requirements Guide*, an authorizing official can revoke authorization, if a cloud service provider fails to comply with FedRAMP requirements.
Establish and implement an incident response and mitigation capability	fully addressed	A Coast Guard official in the Coast Guard Cyber Command stated that the service follows the *Coast Guard Cyber Command Incident Response Plan* for cloud services. The plan outlines activities for implementing a cybersecurity incident response capability and includes guidance on responding to cybersecurity incidents. The *DOD Cloud Computing Security Requirements Guide* requires incidents to be reported to the United States Computer Emergency Readiness Team and DOD, as appropriate.

Security-related federal requirements & guidance	Status	GAO assessment
Follow Trusted Internet Connection requirement	fully addressed	A Coast Guard official in the Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Program Management Office stated that the service's IT systems operate on the Department of Defense Information Network. The network implements Cloud Access Point, which is similar to Trusted Internet Connection.[c] Cloud Access Point is a system of network boundary protection and monitoring devices that cloud service providers use to connect their infrastructure and networks to the Department of Defense Information Network. Cloud Access Point is intended to protect against unauthorized access and malicious activities.
Coordinate with information security and privacy programs	fully addressed	According to the *U.S. Coast Guard Cybersecurity Manual*, the Senior Information Security Officer is responsible for coordinating with the service's Privacy Officer to ensure coordination between information security and privacy programs. The Coast Guard Cyber Command's *Assessment and Authorization Initiation Process Guide*, which outlines the steps for obtaining a system authorization to operate, further defines this responsibility. The process guide specifies that the Information System Security Officer is to coordinate with the service's privacy officers to determine the system privacy requirements and prepare the appropriate privacy documentation, such as the privacy threshold analysis, privacy impact assessment, and system of records notice.[d]
Send the Federal Chief Information Officer a list of cloud services not meeting FedRAMP authorization requirements	Not addressed	Coast Guard officials in the C5I Program Management Office stated that the service did not provide a listing of all cloud services that cannot meet the FedRAMP security authorization requirements, along with the service's rationale and proposed resolution, to the Federal Chief Information Officer. In commenting on a draft of this report, DHS stated that the Coast Guard was initiating a review of all cloud service offerings to ensure that they meet FedRAMP requirements.

Legend:

● = fully addressed: The Coast Guard incorporated the full requirement in its cloud strategy and/or other policies and procedures.

◑ = partially addressed: The Coast Guard incorporated part of the requirement in its cloud strategy and/or other policies and procedures.

○ = not addressed: The Coast Guard had not incorporated the requirement in its cloud strategy or other policies and procedures.

Source: GAO analysis of Coast Guard's documentation. | GAO-22-105092

Note: In January 2017, the Secretaries of DOD and DHS signed an agreement regarding the Coast Guard's cooperation with DOD on cybersecurity and cyberspace operations. That agreement requires the Coast Guard to adhere to DOD cybersecurity requirements, standards, and policies for Coast Guard-operated systems and networks that are on the Department of Defense Information Network. When the Coast Guard's strategy and other cloud-related guidance lacked the required information, we evaluated the DOD strategies and guidance that the Coast Guard is to follow against the identified federal requirements and guidance. For example, we reviewed DOD's *Identity, Credential, and Access Management Strategy*, *Cloud Computing Security Requirements Guide*, and *Cloud Acquisition Guidebook*.

[a] Agile development is a software development model that delivers software in increments throughout the project, but is built iteratively by refining or discarding portions as required based on user feedback.

[b] The FedRAMP Program Management Office developed a security assessment framework that is to be followed by the cloud service providers and agencies seeking to authorize cloud services through the program.

[c] In November 2007, OMB issued M-08-05 that announced the Trusted Internet Connections Initiative. The initiative is intended to improve the federal government's security posture by reducing and consolidating external network connections, including Internet connections, and by centrally monitoring the traffic passing through these connections for potentially malicious activity.

[d] A privacy threshold analysis identifies an IT system and/or technology that involves Personally Identifiable Information, describes what information is collected, and how the information is used.

A privacy impact assessment is an analysis of how personal information is collected, stored, shared, and managed in a federal system. A system of records notice is a formal notice to the public published in the Federal Register that includes the policies and practices of the agency regarding storage, retrievability, and access controls when the agency establishes or makes changes to a system of records.

According to officials in the C5I Program Management Office, the service did not send a list of cloud services that did not meet FedRAMP security authorization requirements to the Federal CIO because it satisfies these requirements through the DOD CIO. Specifically, according to the officials, the Coast Guard's cloud services are required to meet minimum requirements described in the *DOD Cloud Computing Security Requirements Guide*.

In commenting on a draft of this report, DHS stated that the Coast Guard was initiating a review of all cloud service offerings to ensure that they meet FedRAMP requirements. Until the Coast Guard provides notice to the Federal CIO about cloud services that do not meet FedRAMP requirements, the CIO may not have accurate information on whether the service is using FedRAMP approved cloud services.

Coast Guard Incorporated the Procurement-Related Requirements and Guidance

According to the *Federal Cloud Computing Strategy*, the procurement pillar is helpful in improving agencies' ability to purchase cloud solutions through repeatable practices and knowledge sharing. The Coast Guard's cloud strategy and other relevant documentation included all eight procurement-related cloud computing requirements. By having a strategy, policy, or plans that incorporate the procurement-related requirements and guidance, the Coast Guard is better suited to effectively procure cloud services. Table 3 below describes the extent to which the service incorporated procurement related federal cloud computing requirements and guidance in its documentation.

Table 3: Extent Coast Guard Incorporated Procurement-Related Federal Cloud Computing Requirements and Guidance in the Service's Cloud Strategy and Supporting Documentation

Procurement-related federal requirements & guidance	Status	GAO assessment
Oversee IT modernization through the agency Chief Information Officer (CIO)	fully addressed	The *U.S. Coast Guard Cloud Strategy for 2021-2026* describes the principles required to achieve the services priorities for IT modernization. One of those principles is that the CIO facilitate and guide enterprise senior leadership decisions on technology adoption, especially for high-risk, emerging, or non-standard capabilities.
Rationalize the application portfolio	fully addressed	The Coast Guard is to perform application rationalization as part of its biennial investment management process. The service's *Capital Planning and Investment Control Standard Operating Procedures* address the six steps of application rationalization that are described in the *Application Rationalization Playbook* developed by the CIO Council and Cloud & Infrastructure Community of Practice.[a]
Conduct regular evaluations of customer experience and user needs for cloud services	fully addressed	The Coast Guard conducts regular evaluations of the customer experience and user needs through the *Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Operational Analysis Process*. This process is intended to identify whether the service's operational capabilities, programs, and systems, to include cloud services, are meeting requirements and addressing user needs. The operational analysis process is to include in-person site visits and interviews, virtual interviews, and web-based surveys of customer experience and user needs, among other things.
Review the IT portfolio to determine modernization plans	fully addressed	The *Department of Homeland Security (DHS) IT Asset Management and Refresh Policy* requires regular assessment of all Coast Guard IT infrastructure assets to determine whether the assets should be maintained, upgraded, modernized, or replaced. In addition, Coast Guard's *C5I Operational Analysis Process* is intended to continuously monitor the health of deployed C5I capabilities, programs, and systems. Further, solutions in the operations and maintenance phase of the DHS systems engineering life cycle undergo a review to determine whether the solution meets mission outcomes and provides anticipated benefit; validate estimated cost benefits; and provide recommendations on how mission outcomes may be better achieved, among other things.
Establish cloud service level agreements (SLA)	fully addressed	The *DOD Cloud Computing Acquisition Guidebook* requires project managers to define a SLA or use an SLA within a performance work statement as a service delivery summary when acquiring cloud services. The guidebook specifies that SLAs are to include roles and responsibilities of all parties; requirements for cloud service providers to measure performance; and a description of consequences for non-compliance with performance measures, among others.
Ensure continuous visibility of high value assets in cloud service contracts[b]	fully addressed	The *DOD Cloud Acquisition Guidebook* includes a SLA checklist to assist with defining roles and responsibilities for cloud acquisitions, to include those that may be designated as a high value asset. The checklist includes an item to ensure that reporting requirements are outlined in an SLA. The continuous monitoring assessments and reports required by the *DOD Cloud Computing Security Requirements Guide*, in conjunction with reporting requirements outlined by the Coast Guard, would allow the service to have visibility into its cloud acquisitions, including those that are high value assets.

Procurement-related federal requirements & guidance	Status	GAO assessment
Ensure applicable contracts require compliance with the Federal Risk and Authorization Management Program (FedRAMP)	fully addressed	The *DOD Cloud Acquisition Guidebook* includes the required contract language for acquiring cloud services. The guidebook also includes a checklist to assist in developing SLAs for cloud services, which includes an item to ensure that the contract includes provisions to meet all FedRAMP requirements.
Ensure acquisition requirements address upholding FedRAMP requirements, to include contractor reviews and inspections	fully addressed	The *DOD Cloud Computing Security Requirements Guide* outlines a security model for acquiring and maintaining cloud services in accordance with the security authorization requirements set by FedRAMP.[c] Additionally, the *DOD Cloud Acquisition Guidebook* includes contract language requirements related to, among other things, contractor reviews and inspections. For example, the guidebook provides sample contract language requiring cloud service providers to employ an independent third party to conduct an annual security audit based on the federal agency's criteria. The language also includes language that would allow the federal agency to conduct its own audit or investigation.

Legend:

● = fully addressed: The Coast Guard incorporated the full requirement in its cloud strategy and/or other policies and procedures.

◑ = partially addressed: The Coast Guard incorporated part of the requirement in its cloud strategy and/or other policies and procedures.

○ = not addressed: The Coast Guard had not incorporated the requirement in its cloud strategy or other policies and procedures.

Source: GAO analysis of Coast Guard's documentation. | GAO-22-105092

Note: In January 2017, the Secretaries of DOD and DHS signed an agreement regarding the Coast Guard's cooperation with DOD on cybersecurity and cyberspace operations. That agreement requires the Coast Guard to adhere to DOD cybersecurity requirements, standards, and policies for Coast Guard-operated systems and networks that are on the Department of Defense Information Network. When the Coast Guard's strategy and other cloud-related guidance lacked the required information, we evaluated the DOD strategies and guidance that the Coast Guard is to follow against the identified federal requirements and guidance. For example, we reviewed DOD's *Identity, Credential, and Access Management Strategy*, *Cloud Computing Security Requirements Guide*, and *Cloud Acquisition Guidebook*.

[a] The six-step process for application rationalization includes: 1) identify needs and establish a business case; 2) inventory and capture relevant information; 3) assess the business value and technical fit; 4) assess the current-state total cost of ownership for the applications against the future-state architectures; 5) score applications; and 6) execute a change management and application migration strategy.

[b] A high value asset is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business.

[c] According to the *FedRAMP Security Assessment Framework*, the cloud service providers are required to maintain FedRAMP authorization by conducting continuous monitoring.

Coast Guard Varied in its Incorporation of the Workforce-Related Requirements and Guidance

According to the *Federal Cloud Computing Strategy*, the workforce pillar will help to train and recruit key talent for cybersecurity, acquisition, and cloud engineering. Of the four workforce-related cloud computing requirements, the Coast Guard's cloud strategy and other relevant documentation fully included two, and partially included two workforce-related requirements and guidance. Table 4 below describes the extent to which the service incorporated workforce-related federal cloud computing requirements and guidance in its documentation.

Table 4: Extent Coast Guard Incorporated Workforce Related Federal Cloud Computing Requirements and Guidance in the Service's Cloud Strategy and Supporting Documentation

Workforce-related federal requirements & guidance	Status	GAO assessment
Provide cloud-related and other relevant training	fully addressed	One of the guiding principles identified in the service's cloud strategy states that the service will provide ongoing training to keep pace with industry trends and recruit staff to ensure mission readiness. The Coast Guard also makes training available to its IT workforce in the areas of cloud concepts, architecture, and design; cloud data and application security; and cloud platform and infrastructure security. Further, the Coast Guard makes training available to its staff in the areas of lean product management, agile development, continuous delivery, and automated infrastructure. A Coast Guard official in the Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Program Management Office stated that this training is made available to its staff, regardless of their job title or role.
Execute communication plans	fully addressed	The *DOD 365 Communications Action Plan* is intended to serve as a baseline framework to foster awareness, educate users on upcoming changes, and promote adoption and change of cloud technologies. The plan includes milestones and talking points that are intended to help the employees understand what changes will occur, and provide learning opportunities that are available.
Establish a strategy for workforce development, to include a cross-walk of new and old skills and occupational categories	partially addressed	The *U.S. Coast Guard Human Capital Strategy* states that the service is to use existing competency structures to assess the similarities between new requirements and existing workforce skills. In addition, one of the objectives outlined in the *U.S. Coast Guard Cloud Strategy for 2021-2026* is to develop cloud expertise in the service's workforce by, among other things, investing in workforce development. A Coast Guard official in the C5I Program Management Office stated that the service conducted an initial cyber workforce analysis in 2017, which led to changes in required competencies and specialty codes. However, the aforementioned strategies did not describe the service's plans to perform a crosswalk of new skills and occupational categories with legacy occupational categories as the service transitions to a cloud environment.
Conduct cloud-based skills gap analysis	partially addressed	The *U.S. Coast Guard Cloud Strategy for 2021-2026* and other relevant documentation did not address the requirement to conduct a cloud-based skills gap analyses. Despite that, the Coast Guard officials stated that it conducted a workforce gap analysis in April 2021, but the analysis report was limited—focusing on the Information Systems Security Officer and Assistant Information Systems Security Officer positions. In addition, the analysis did not include information related to the service's transition to cloud services. The Coast Guard plans to conduct a workforce analysis in fiscal year 2022, but this analysis will focus only on the Coast Guard Cyber Command and not other Coast Guard units that perform IT-related tasks.

Legend:

● = fully addressed: The Coast Guard incorporated the full requirement in its cloud strategy and/or other policies and procedures.

◑ = partially addressed: The Coast Guard incorporated part of the requirement in its cloud strategy and/or other policies and procedures.

○ = did not address: The Coast Guard had not incorporated the requirement in its cloud strategy or other policies and procedures.

Source: GAO analysis of Coast Guard's documentation. | GAO-22-105092

Note: In January 2017, the Secretaries of DOD and DHS signed an agreement regarding the Coast Guard’s cooperation with DOD on cybersecurity and cyberspace operations. That agreement requires the Coast Guard to adhere to DOD cybersecurity requirements, standards, and policies for Coast Guard-operated systems and networks that are on the Department of Defense Information Network.

When the Coast Guard’s strategy and other cloud-related guidance lacked the required information, we evaluated the DOD strategies and guidance that Coast Guard is to follow against the identified federal requirements and guidance. For example, we reviewed DOD’s *Identity, Credential, and Access Management Strategy*, *Cloud Computing Security Requirements Guide*, and *Cloud Acquisition Guidebook*.

In April 2022, a Coast Guard official in the Office of Cyberspace Forces stated that the service had received funding to conduct a workforce analysis on the Coast Guard Cyber Command during fiscal year 2022, and that those efforts were underway. According to officials in the same office’s Resources and Planning division, the analysis is scheduled to begin in May 2022 and be completed by May 2023. An official in the C5I Program Management Office stated that the analysis is intended to determine how best to align, manage, and standardize cyberspace work roles, baseline qualifications, and training requirements, and may inform the development of new occupational categories as the service transitions to a cloud environment. However, the official expected that the workforce analysis would focus on the service’s Cyber Command and not other units that perform IT-related tasks. In January 2022, officials in the Office of Cyberspace Forces noted that it was not planning to perform a workforce analysis of the entire cyberspace workforce due to the widely distributed and diverse nature of the service’s units that have staff that make up the cyberspace workforce.

Until the Coast Guard updates its cloud strategy and other relevant documentation, to fully address a workforce development strategy that incorporates a cross-walk of new and old skills as the service transitions to a cloud environment and a cloud-based skills gap analysis for the entire Coast Guard cyberspace workforce, the service has limited assurance that it has the skilled staff necessary to successfully support cloud adoption.

Conclusions

Effective management of the Coast Guard’s IT program is essential for improving the productivity, efficiency, and effectiveness of the programs supporting the service’s important missions. While the Coast Guard has implemented processes to address its IT resources, it lacks a documented network capacity planning process, a key component of IT infrastructure planning. Without planning for adequate network capacity, the Coast Guard accepts substantial risks in resulting inefficiencies and disruptions in network availability to users.

In addition, the Coast Guard has documented a cybersecurity risk management process that describes how the service is to select, identify, and assess security controls for IT and some operational technology. Nevertheless, the Coast Guard did not consistently apply its cybersecurity risk management process for platform IT. Further, the process is not comprehensive because it does not include two types of operational technology—ICS and SCADA. Accordingly, the Coast Guard cannot ensure that it is effectively managing risks to all systems.

The Coast Guard developed a cloud strategy that outlines its strategic objectives for cloud computing and describes the service's priorities for IT modernization efforts over the next five years. The strategy and other supporting documentation addressed most of the federal cloud computing requirements and guidance, but did not include key actions related to cloud security and its workforce. Updating its strategy to include all cloud-related requirements and guidance would further facilitate the migration to cloud services.

Recommendations for Executive Action

We are making the following eight recommendations to the Coast Guard:

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to develop network capacity planning policies and procedures that address the leading practices we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs. (Recommendation 1)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to implement the leading practices for network capacity planning that we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and

(5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs. (Recommendation 2)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to establish a comprehensive and accurate inventory of all operational technology, including ICS and SCADA systems. (Recommendation 3)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to develop a plan or strategy for aligning all operational technology to the Department of Defense risk management framework, including time frames for completing the alignment. (Recommendation 4)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to ensure that the plan or strategy for aligning all operational technology to the Department of Defense risk management framework is effectively implemented. (Recommendation 5)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to update existing policies and procedures to explicitly describe a cybersecurity risk management process for ICS and SCADA systems. (Recommendation 6)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to send its list of cloud services that do not meet FedRAMP requirements to the appropriate agency head for submission to the Federal CIO. (Recommendation 7)

The Commandant of the United States Coast Guard should direct the Deputy Commandant for Mission Support to update the service’s cloud strategy and other relevant documentation to include a cross-walk of new and old skills and occupational categories, and to conduct a skills gap analysis. (Recommendation 8)

Agency Comments

We provided a draft of this report to DHS for comment. In its comments, reproduced in appendix IV, DHS concurred with all eight recommendations. The department recognized the importance of having improved IT management and OT processes and managing risks for all systems. In its response, the department included actions it plans to take to address each recommendation. The Coast Guard also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of the Department of Homeland Security, the Commandant of the Coast Guard, 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 (404) 679-1831 or FranksJ@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Jennifer R. Franks
Director, Information Technology and Cybersecurity

Appendix I: Objectives, Scope, and Methodology

Our specific objectives were to determine (1) the extent to which the Coast Guard has a process to ensure its IT infrastructure meets its current needs, including planning for network capacity; (2) the Coast Guard's cybersecurity risk management process for information technology and how, if at all, the process differs for operational technology; and (3) the extent to which the Coast Guard has incorporated federal requirements and guidance in its strategy for implementing cloud computing.

To address the first objective, we reviewed and summarized documentation describing the Coast Guard's processes to ensure the adequacy of the service's IT infrastructure to meet mission needs. The documentation included the *Department of Homeland Security (DHS) IT Asset Management and Refresh Policy* and *Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Operational Analysis Process*.

We also assessed the service's efforts to plan for adequate network capacity. To do this, we identified common practices for network capacity planning by collecting and reviewing publicly available federal and industry guidance. Our searches of publicly available data regarding network capacity planning resulted in:

- guidance from two federal agencies—the Internal Revenue Service and Centers for Disease Control and Prevention;
- industry whitepapers from Cisco and SolarWinds—technology-based corporations that provide IT products and services to the federal government and others; and
- articles on network capacity planning from IT-focused organizations, such as Comparitech and Computerworld.

We analyzed and compared the information provided from each resource and identified the following five common practices for network capacity planning:

1. compile a hardware, software, and configuration inventory;

2. identify the baseline network utilization and traffic growth predictions;
3. determine bandwidth allocation needs for variations and prioritize network traffic;
4. run simulations and what-if analyses; and
5. make refinements to the network and continually monitor the health of the network.

We then analyzed documentation of the service's efforts to plan for adequate network capacity. The documentation included hardware, software, and configuration inventories; analysis reports and screenshots from network monitoring tools; the *July 2020 U.S. Coast Guard IT Asset Refresh Implementation Report*; and an operational assessment report on the service's IT infrastructure and network. We compared this documentation to the common practices we identified for network capacity planning to determine the extent to which the Coast Guard's processes addressed them.

Further, we reviewed operational assessment reports related to the Coast Guard's IT capabilities between October 2020 and September 2021 to identify any performance issues or user challenges.[1] We supplemented our analyses by interviewing relevant Coast Guard officials in the C5I Program Management Office and C5I Service Center to obtain information about the service's processes and efforts for network capacity planning.

To address the second objective, we reviewed cybersecurity risk management policies and procedures, such as the *U.S. Coast Guard Cybersecurity Manual*, the Risk Management Framework for Department of Defense (DOD) IT, and *DHS Sensitive Systems Handbook*, to determine how the service is to apply cybersecurity risk management for IT and operational technology. We also reviewed documentation, such as the Coast Guard's August 2021 *Cyber Strategic Outlook*, to understand how the service defines operational technology. Using these policies and procedures, we then compared the Coast Guard's risk management

[1] Operational assessments are intended to identify user satisfaction and information regarding the effectiveness of capabilities deployed by C5I. The results of the assessments are documented in a report that is used to inform decision making and meet investment management reporting requirements.

processes for IT and operational technology, determined whether the processes differed, and summarized both processes.

To determine if the service was following its cybersecurity risk management process for operational technology, we selected a sample of systems listed as platform IT (one type of operational technology) in the Coast Guard's Enterprise Systems Inventory (ESI).[2] Using ESI, we identified Coast Guard-owned systems designated as platform IT, and sorted the resulting list of systems based on the Federal Information Processing Standards security categorizations—high-, moderate-, and low-impact—and other data entries for the security categorization data element (i.e., to be determined and not applicable).[3] Within each group of available security categorization entries—excluding low-impact—we listed the systems in the order that they appeared in ESI, assigned each system a consecutive number, and used a random number generator to select systems based on the number they were assigned. In doing so, we selected:

- two systems that were high-impact;
- two systems that were moderate-impact;
- two systems that had "to be determined" listed in the security categorization, and were also designated as a major information system in the inventory; and
- one system with "not applicable" for the security categorization.

[2] Coast Guard officials stated that, in addition to platform IT, the service also considers platform IT systems, industrial control systems (ICS), and supervisory control and data acquisition systems (SCADA) as operational technology. However, ESI's data element for platform IT did not distinguish between platform IT and platform IT systems, and the service did not maintain an inventory of ICS and SCADA. Therefore, our sample of operational technology consisted only of those designated as "platform IT."

[3] Information systems are categorized according to the magnitude of harm or impact resulting from the system or its information being compromised. The *Standards for Security Categorization of Federal Information and Information Systems* define three impact levels where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (low), a serious adverse effect (moderate), or a severe or catastrophic adverse effect (high) on organizational operations, organizational assets, or individuals. *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, Md.: February 2004).

We also selected the one system in ESI that included blank information for the security categorization data element. Our methodology resulted in the selection of eight systems.

We analyzed available system security authorization documentation for each selected system to determine how the Coast Guard applied its cybersecurity risk management process for those systems. The documentation we analyzed included system risk assessments, system security plans, security assessment reports, and plans of action and milestones. Specifically, if the required documentation was available, we compared them to process guides for implementing the service's risk management process. These guides included the *Assessment and Authorization (A&A) Initiation Process Guide*, *Platform IT Process Guide*, and *Reciprocity Process Guide*. We supplemented our analysis by interviewing relevant officials in the Coast Guard's Assistant Commandant for Command, Control, Communications, Computers, and IT and the Coast Guard's Cyber Command to obtain further information on how the service defines operational technology and the service's cybersecurity risk management process.

To address the third objective, we identified federal cloud computing requirements and guidance, including those contained in the Office of Management and Budget (OMB)'s *Federal Cloud Computing Strategy* and memorandum on *Security Authorization of Information Systems in Cloud Computing Environments*, and the President's Executive Order on *Improving the Nation's Cybersecurity*.[4] We then summarized the requirements and guidance, excluding actions that were conveyed as good practices (i.e., they did not use language such as "should," "must," or "are required to"). We also excluded actions that were irrelevant to the Coast Guard, such as those directed to the agency head (DHS) and not a component agency. We grouped the final list of requirements and guidance into the three pillars outlined in OMB's *Federal Cloud Computing Strategy*—security, procurement, and workforce.

We compared the Coast Guard's cloud strategy and other related guidance to the list of requirements we grouped into the three pillars to determine whether they described the service's efforts to implement the

[4] *Executive Order on Improving the Nation's Cybersecurity* (May 2021)*;* Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019); OMB, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

requirements for cloud computing that we identified. Specifically, we evaluated

- *U.S. Coast Guard's Cloud Strategy for 2021–2026,*
- *Information Systems Security Officer New Performance Planning Front End Analysis,*
- *Coast Guard Incident Response Plan,*
- *CG-6 Capital Planning and Investment Control Standard Operating Procedures,*
- *C5I Investment Business Case Evaluation and Review Process, and*
- *C5I Operational Analysis Process*.

To supplement our review of the Coast Guard's strategy and other cloud-related guidance, we also evaluated the DOD strategies and guidance that the Coast Guard is to follow.[5] For example, we reviewed DOD's *Identity, Credential, and Access Management Strategy*, *Cloud Computing Security Requirements Guide*, and *Cloud Acquisition Guidebook*. We also compared this documentation against the identified federal requirements and guidance when the Coast Guard's documentation lacked the required information.

We supplemented our analyses by interviewing relevant Coast Guard officials in the C5I Program Management Office, the Office of Cyberspace Forces, and the Assistant Commandant for Acquisition to determine the status of ongoing cloud migrations and obtain information on future plans for cloud computing at the service. We also interviewed the officials to identify challenges that the service has with cloud computing.

We conducted this performance audit from March 2021 to July 2022 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.

[5] In January 2017, the Secretaries of DOD and DHS signed an agreement regarding the Coast Guard's cooperation with DOD on cybersecurity and cyberspace operations. That agreement requires the Coast Guard to adhere to DOD cybersecurity requirements, standards, and policies for Coast Guard-operated systems and networks that are on the Department of Defense Information Network.

Appendix II: Federal Requirements and Guidance for Cloud Computing

In December 2011, the Office of Management and Budget (OMB) issued a memo on *Security Authorization of Information Systems in Cloud Computing Environments*, which sets policy for federal agencies to protect information in the cloud through adoption of the Federal Risk and Authorization Management Program—commonly known as FedRAMP.[1] Additionally, in June 2019, OMB issued the *Federal Cloud Computing Strategy* that includes requirements and guidance for federal agencies to implement cloud computing.[2] The strategy outlines three key pillars—security, procurement, and workforce—that are intended to assist agencies in successful cloud adoption. We categorized the requirements and guidance described in the aforementioned federal documents into areas based on the three key pillars outlined in OMB's *Federal Cloud Computing Strategy*. Table 5 below provides a detailed description of the federal requirements and guidance supporting each of the three areas.

Table 5: Cloud Computing Requirements and Guidance in the Areas of Security, Procurement, and Workforce

Area	Key Requirement	Description
Security	Implement identity, credential, and access management	Implement Identity, Credential, and Access Management to continuously protect data and provide awareness in cloud-based environments.
	Use mature agile development practices	Agencies should utilize mature agile development practices, including development, security, and operations to realize the security benefits of cloud infrastructure and scalability.[a]
	Perform continuous monitoring	Agencies should perform continuous monitoring to detect malicious activity and dedicate effort to improving systems governance.
	Update business continuity and disaster recovery plans	Agencies should update business continuity and disaster recovery plans to include contingencies involving the sudden interruption or termination of cloud services.
	Secure cloud environments	Agencies should take a risk-based approach to securing cloud environments by placing an emphasis on protections at the data layer, in addition to the network and physical infrastructure layers; transitioning to a multi-layer defense strategy (also known as defense-in-depth).

[1] Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Washington, D.C.: Dec. 8, 2011).

[2] Office of Management and Budget, *Federal Cloud Computing Strategy* (Washington, D.C.: June 24, 2019).

Area	Key Requirement	Description
	Use the Federal Risk and Authorization Management Program (FedRAMP)	Use the FedRAMP Program Management Office requirements as a baseline when conducting risk assessments and security authorizations, granting an authorization to operate, and revoking security authorizations for the agency's use of cloud services.
	Establish and implement an incident response and mitigation capability	Establish and implement an incident response and mitigation capability for security and privacy incidents for cloud services in accordance with the Department of Homeland Security (DHS) guidance.
	Follow Trusted Internet Connection requirements	Consistent with DHS guidance, require that cloud service providers route their traffic such that the service meets the requirements of the Trusted Internet Connection program.[b]
	Coordinate with information security and privacy programs	Coordination between information security and privacy programs is necessary to ensure compliance with applicable privacy requirements and for the successful identification and management of risks to individuals when processing personally identifiable information.
	Send the Federal Chief Information Officer a list of cloud services not meeting FedRAMP authorization requirements	Provide to the Federal Chief Information Officer (CIO) annually on April 30, a certification in writing from the executive department or agency CIO and Chief Financial Officer, a listing of all cloud services that an agency determines cannot meet the FedRAMP security authorization requirements with appropriate rationale and proposed resolutions.
Procurement	Oversee IT modernization through the agency Chief Information Officer	The agency CIO should oversee modernization processes to help identify opportunities for enterprise-wide improvement.
	Rationalize the application portfolio	All federal agencies are to rationalize their application portfolios to drive federal cloud adoption. The rationalization process involves reducing an application portfolio by 1) assessing the need for and usage of applications; and 2) discarding obsolete, redundant, or overly resource-intensive applications. Agencies should regularly rationalize and update their applications.
	Conduct regular evaluations of customer experience and user needs for cloud services	Agencies should conduct regular evaluations of customer experience and user needs to ensure that their solutions successfully foster efficiency, accessibility, and privacy.
	Review the IT portfolio to determine modernization plans	Agencies should review their IT portfolios regularly to determine modernization plans for existing tools.
	Establish cloud service level agreements (SLA)	Where a cloud solution is deployed by a vendor, agencies should ensure that a SLA be in place that provides the agency with continuous awareness of the confidentiality, integrity, and availability of its information. The SLA should include: • notifying the agency of a confirmed or suspected cybersecurity incident; • providing continuous access to log data; • articulating roles and responsibilities; • establishing clear performance metrics; and • implementing remediation plans for non-compliance with the service level agreement.
	Ensure continuous visibility of high value assets in cloud service contracts	Agencies must ensure that contracts impacting their high value assets, including those managed and operated in the cloud, include requirements that provide agencies with continuous visibility of the asset.
	Ensure that applicable contracts require compliance with FedRAMP requirements	Ensure applicable contracts appropriately require cloud service providers to comply with FedRAMP security authorization requirements.

Area	Key Requirement	Description
	Ensure acquisition requirements address upholding FedRAMP requirements, to include contractor reviews and inspections	Ensure that acquisition requirements address upholding FedRAMP security authorization requirements and that relevant contract provisions related to contractor reviews and inspections are included for cloud service providers.
Workforce	Provide cloud-related and other relevant training	Agency IT staff should become familiar with lean product management, agile development, continuous delivery, and automated infrastructure. Additionally, non-IT staff supporting privacy, security, and procurement should receive training in these areas. Agencies should plan for ongoing education in this rapidly evolving field.
	Execute communication plans regarding changes affecting employees	Agencies should execute communication plans that help employees understand the changes that will occur, and an outline of the change management process to include reskilling opportunities that will be helpful for the employees.
	Establish a strategy for workforce development, to include a cross-walk of new and old skills and occupational categories	Agencies' cloud strategies and policies should include a workforce development and planning component that tailors a transformation and training approach to that agency. In the event that an impact to the existing workforce has been identified, this approach should include a cross-walk of new skills and occupational categories with legacy occupational categories to foster clarity and ease of transition.
	Conduct cloud-based skills gap analyses for future skill and position requirements	Agency Chief Information Officers, Chief Human Capital Officers, and Senior Agency Officials for Privacy should collaboratively conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements. Agencies should identify potential skills gaps that emerge as a result of a transition to cloud-based services, and, where needed, equip their existing staff with additional skills and knowledge to keep up with the ever-expanding list of technology options available to procure and deploy.

Source: GAO analysis of federal requirement and guidance related to cloud computing. | GAO-22-105092

[a] Agile development is a software development model that delivers software in increments throughout the project, but is built iteratively by refining or discarding portions as required based on user feedback.

[b] In November 2007, OMB issued M-08-05 that announced the Trusted Internet Connections Initiative. The initiative is intended to improve the federal government's security posture by reducing and consolidating external network connections, including Internet connections, and by centrally monitoring the traffic passing through these connections for potentially malicious activity.

Appendix III: Status of Coast Guard's Completed and Planned Cloud Migrations

As of April 2022, the Coast Guard deployed four cloud services and was in the process of transitioning to three additional cloud services. Table 6 shows the status of each of the cloud services. A Coast Guard official in the Command, Control, Communications, Computers, Cyber, and Intelligence Program Management Office stated, in December 2021, that the service had recently been awarded two cloud contracts—one for a budget formulation tool and another for an enterprise architecture tool.

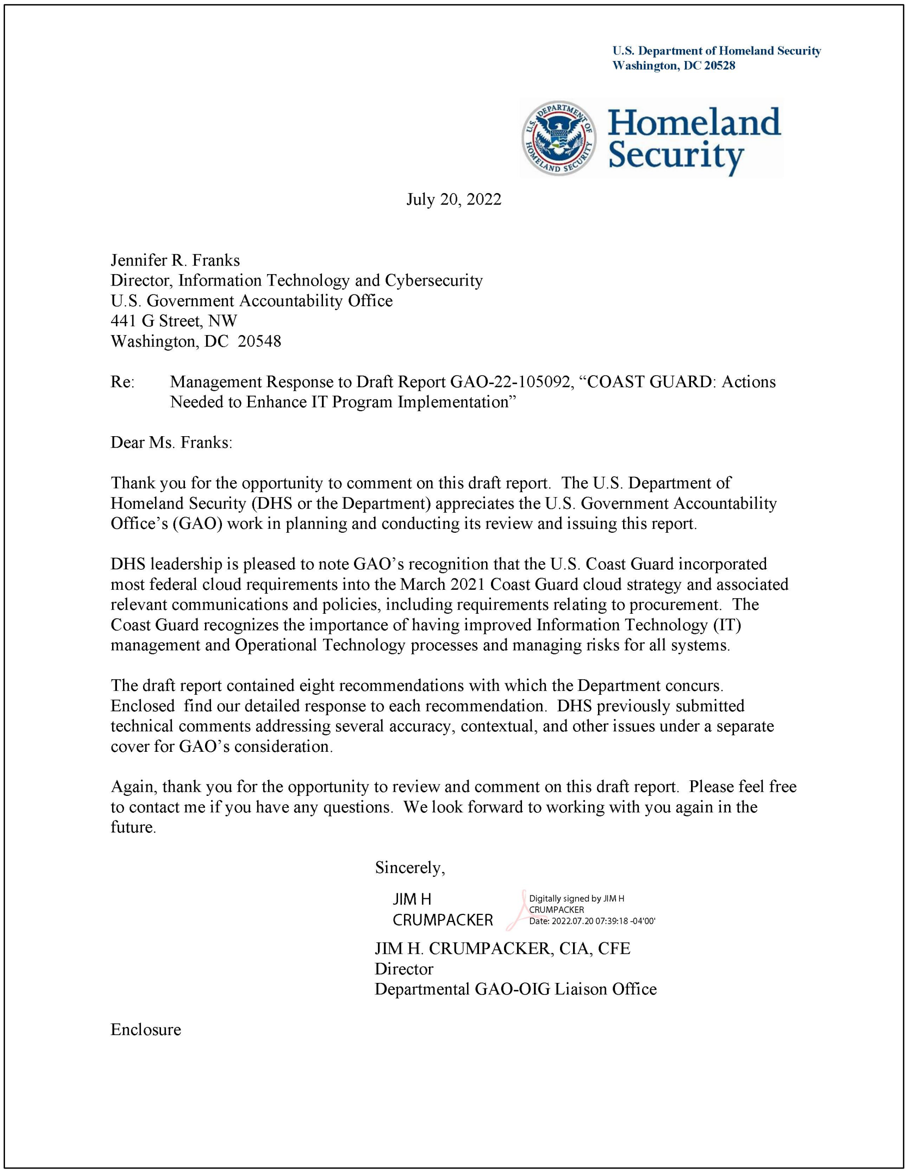
Table 6: Status of Coast Guard's Planned and Implemented Cloud Services as of April 2022

Cloud Services	Planned (Final Operational Capability)	Completed (Final Operational Capability)
AUXDATA The Coast Guard's repository for personnel, program, and activity data for the service's active and retired members.	June 2020	June 2020
Video Enabled Telehealth A secure, privacy-compliant telehealth video conferencing system that would provide Coast Guard members with remote access to a wide range of health care services.	4th quarter fiscal year 2021	June – July 2021
Department of Defense (DOD) 365 A solution for on-site and remote office productivity and collaboration. The Coast Guard is implementing DOD365, which includes an integrated voice, video, and chat platform with file sharing, cloud storage, and productivity applications. *Microsoft Teams* Cloud based collaborative application that helps users to schedule meetings, conduct phone calls, share files, and send instant messages. *OneDrive* A repository to store files which enable users to access, share, and collaborate on Word documents, Excel spreadsheets, and PowerPoint presentations in real time. *Microsoft SharePoint* A web-based collaborative platform the helps organizations share and manage content, knowledge, and applications.	September 2021 November 2021 December 2022	September 2021 November 2021 Pending completion
Recruiting Case Management A tool to manage the Coast Guard's recruiting process.	July 2022	Pending completion

Cloud Services	Planned (Final Operational Capability)	Completed (Final Operational Capability)
Maritime Analytic Support System An all source intelligence system comprised of analytic, visualization, and database components.	May 2024	Pending completion

Source: GAO analysis of Coast Guard documentation. | GAO-22-105092

Appendix IV: Comments from the U.S. Coast Guard



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

Homeland Security

July 20, 2022

Jennifer R. Franks
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-105092, "COAST GUARD: Actions Needed to Enhance IT Program Implementation"

Dear Ms. Franks:

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

DHS leadership is pleased to note GAO's recognition that the U.S. Coast Guard incorporated most federal cloud requirements into the March 2021 Coast Guard cloud strategy and associated relevant communications and policies, including requirements relating to procurement. The Coast Guard recognizes the importance of having improved Information Technology (IT) management and Operational Technology processes and managing risks for all systems.

The draft report contained eight recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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.

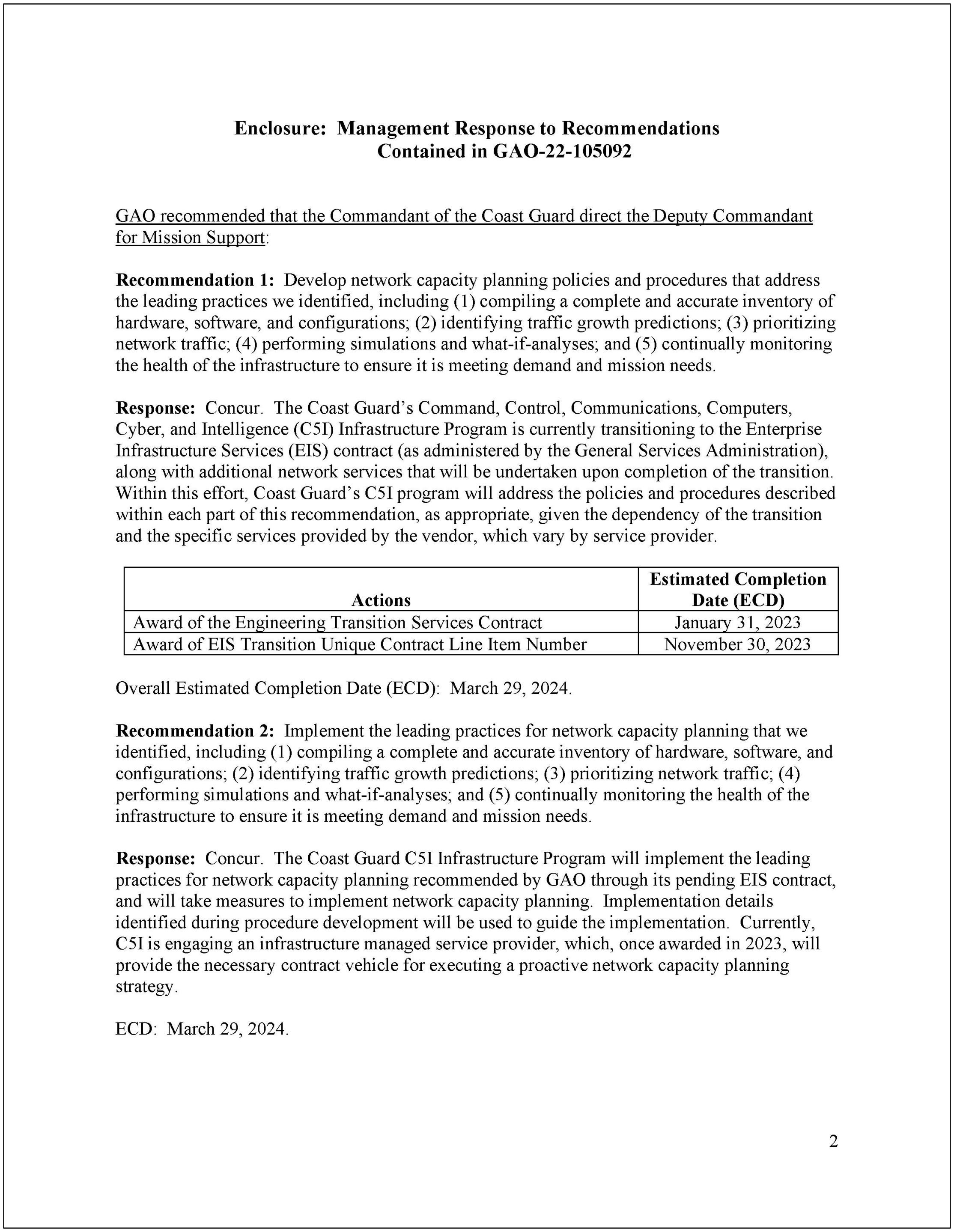
Sincerely,

JIM H
CRUMPACKER

Digitally signed by JIM H
CRUMPACKER
Date: 2022.07.20 07:39:18 -04'00'

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

Enclosure



Enclosure: Management Response to Recommendations Contained in GAO-22-105092

GAO recommended that the Commandant of the Coast Guard direct the Deputy Commandant for Mission Support:

Recommendation 1: Develop network capacity planning policies and procedures that address the leading practices we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs.

Response: Concur. The Coast Guard's Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Infrastructure Program is currently transitioning to the Enterprise Infrastructure Services (EIS) contract (as administered by the General Services Administration), along with additional network services that will be undertaken upon completion of the transition. Within this effort, Coast Guard's C5I program will address the policies and procedures described within each part of this recommendation, as appropriate, given the dependency of the transition and the specific services provided by the vendor, which vary by service provider.

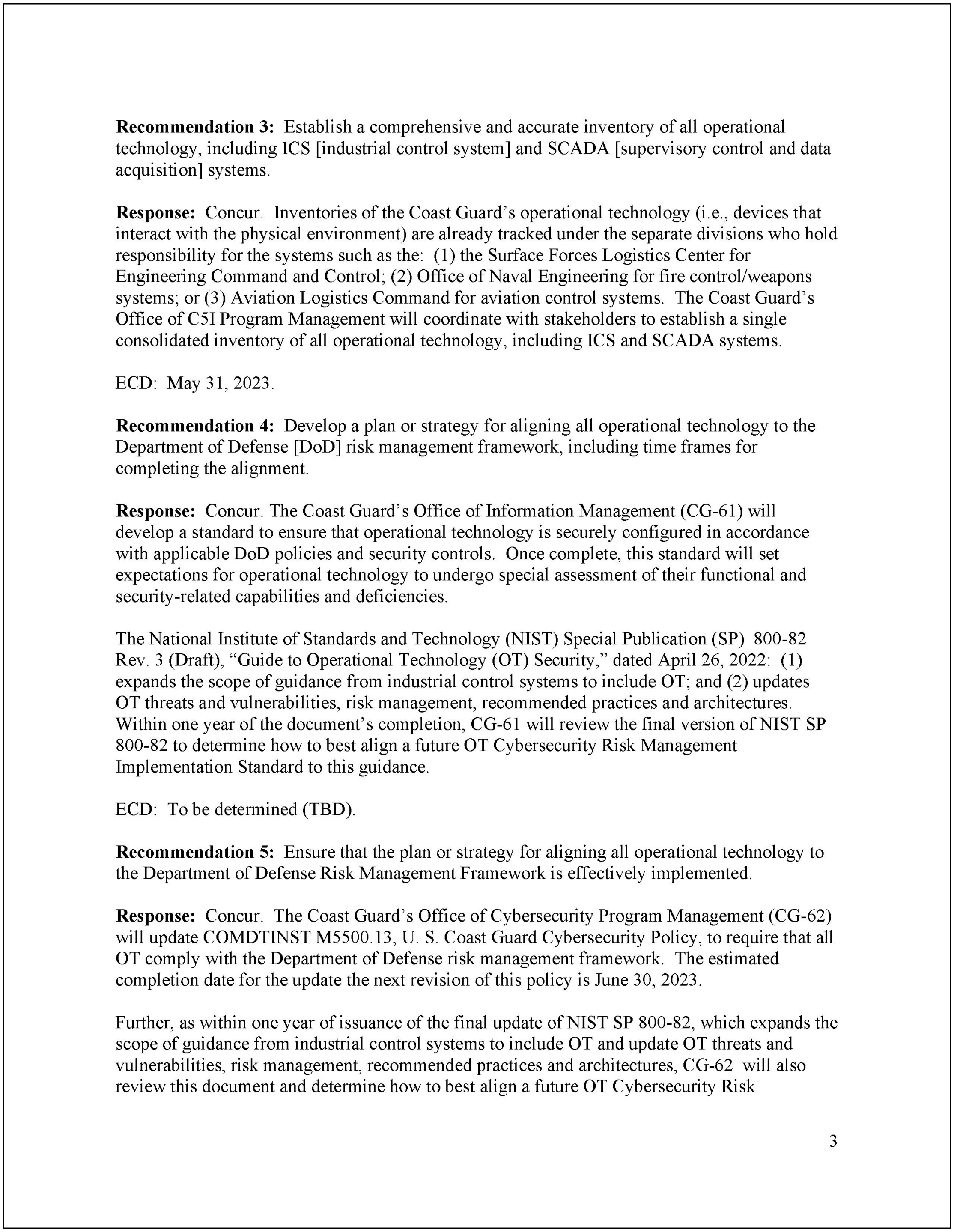
Actions	Estimated Completion Date (ECD)
Award of the Engineering Transition Services Contract	January 31, 2023
Award of EIS Transition Unique Contract Line Item Number	November 30, 2023

Overall Estimated Completion Date (ECD): March 29, 2024.

Recommendation 2: Implement the leading practices for network capacity planning that we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs.

Response: Concur. The Coast Guard C5I Infrastructure Program will implement the leading practices for network capacity planning recommended by GAO through its pending EIS contract, and will take measures to implement network capacity planning. Implementation details identified during procedure development will be used to guide the implementation. Currently, C5I is engaging an infrastructure managed service provider, which, once awarded in 2023, will provide the necessary contract vehicle for executing a proactive network capacity planning strategy.

ECD: March 29, 2024.



Recommendation 3: Establish a comprehensive and accurate inventory of all operational technology, including ICS [industrial control system] and SCADA [supervisory control and data acquisition] systems.

Response: Concur. Inventories of the Coast Guard's operational technology (i.e., devices that interact with the physical environment) are already tracked under the separate divisions who hold responsibility for the systems such as the: (1) the Surface Forces Logistics Center for Engineering Command and Control; (2) Office of Naval Engineering for fire control/weapons systems; or (3) Aviation Logistics Command for aviation control systems. The Coast Guard's Office of C5I Program Management will coordinate with stakeholders to establish a single consolidated inventory of all operational technology, including ICS and SCADA systems.

ECD: May 31, 2023.

Recommendation 4: Develop a plan or strategy for aligning all operational technology to the Department of Defense [DoD] risk management framework, including time frames for completing the alignment.

Response: Concur. The Coast Guard's Office of Information Management (CG-61) will develop a standard to ensure that operational technology is securely configured in accordance with applicable DoD policies and security controls. Once complete, this standard will set expectations for operational technology to undergo special assessment of their functional and security-related capabilities and deficiencies.

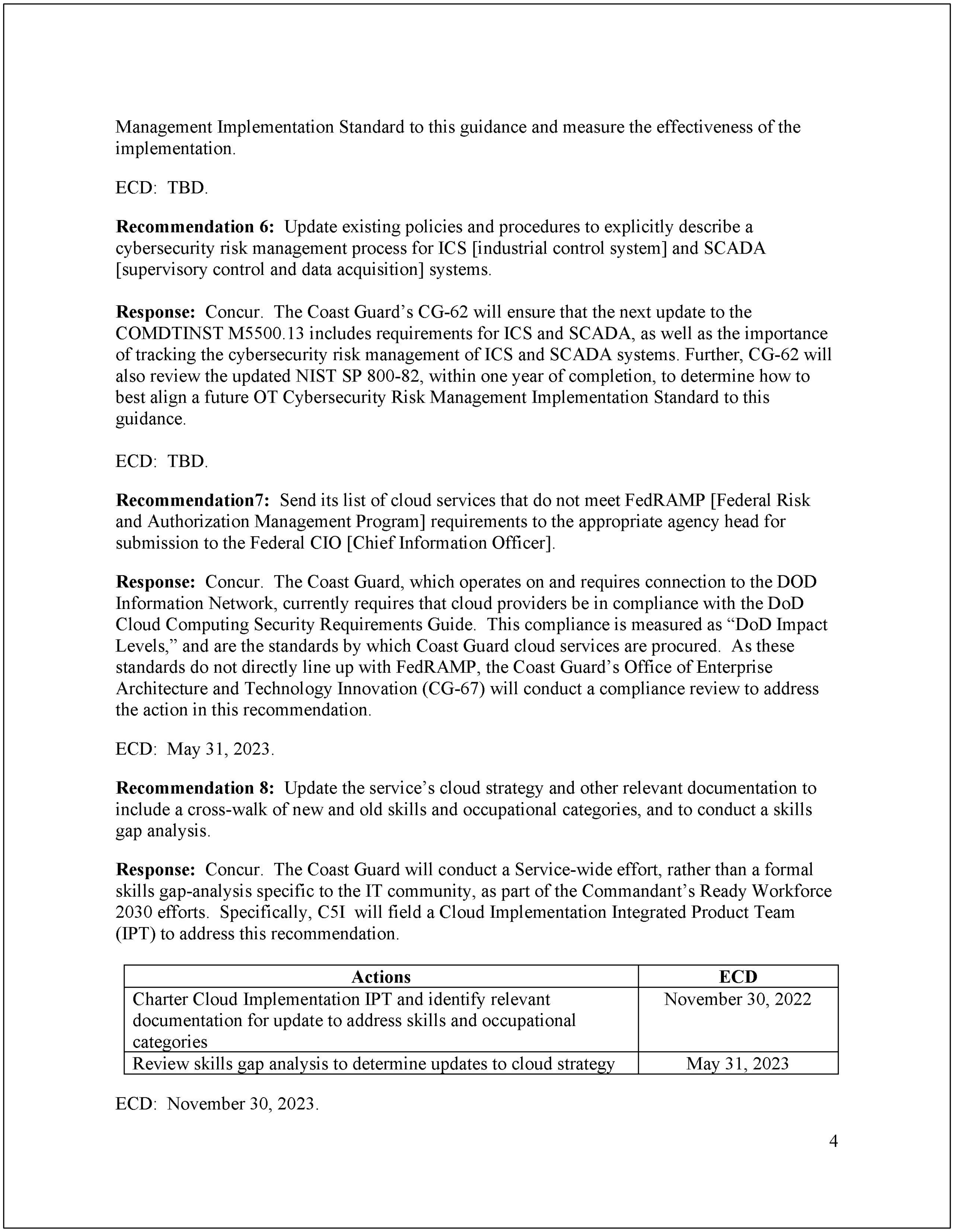
The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 3 (Draft), "Guide to Operational Technology (OT) Security," dated April 26, 2022: (1) expands the scope of guidance from industrial control systems to include OT; and (2) updates OT threats and vulnerabilities, risk management, recommended practices and architectures. Within one year of the document's completion, CG-61 will review the final version of NIST SP 800-82 to determine how to best align a future OT Cybersecurity Risk Management Implementation Standard to this guidance.

ECD: To be determined (TBD).

Recommendation 5: Ensure that the plan or strategy for aligning all operational technology to the Department of Defense Risk Management Framework is effectively implemented.

Response: Concur. The Coast Guard's Office of Cybersecurity Program Management (CG-62) will update COMDTINST M5500.13, U. S. Coast Guard Cybersecurity Policy, to require that all OT comply with the Department of Defense risk management framework. The estimated completion date for the update the next revision of this policy is June 30, 2023.

Further, as within one year of issuance of the final update of NIST SP 800-82, which expands the scope of guidance from industrial control systems to include OT and update OT threats and vulnerabilities, risk management, recommended practices and architectures, CG-62 will also review this document and determine how to best align a future OT Cybersecurity Risk



Management Implementation Standard to this guidance and measure the effectiveness of the implementation.

ECD: TBD.

Recommendation 6: Update existing policies and procedures to explicitly describe a cybersecurity risk management process for ICS [industrial control system] and SCADA [supervisory control and data acquisition] systems.

Response: Concur. The Coast Guard's CG-62 will ensure that the next update to the COMDTINST M5500.13 includes requirements for ICS and SCADA, as well as the importance of tracking the cybersecurity risk management of ICS and SCADA systems. Further, CG-62 will also review the updated NIST SP 800-82, within one year of completion, to determine how to best align a future OT Cybersecurity Risk Management Implementation Standard to this guidance.

ECD: TBD.

Recommendation7: Send its list of cloud services that do not meet FedRAMP [Federal Risk and Authorization Management Program] requirements to the appropriate agency head for submission to the Federal CIO [Chief Information Officer].

Response: Concur. The Coast Guard, which operates on and requires connection to the DOD Information Network, currently requires that cloud providers be in compliance with the DoD Cloud Computing Security Requirements Guide. This compliance is measured as "DoD Impact Levels," and are the standards by which Coast Guard cloud services are procured. As these standards do not directly line up with FedRAMP, the Coast Guard's Office of Enterprise Architecture and Technology Innovation (CG-67) will conduct a compliance review to address the action in this recommendation.

ECD: May 31, 2023.

Recommendation 8: Update the service's cloud strategy and other relevant documentation to include a cross-walk of new and old skills and occupational categories, and to conduct a skills gap analysis.

Response: Concur. The Coast Guard will conduct a Service-wide effort, rather than a formal skills gap-analysis specific to the IT community, as part of the Commandant's Ready Workforce 2030 efforts. Specifically, C5I will field a Cloud Implementation Integrated Product Team (IPT) to address this recommendation.

Actions	ECD
Charter Cloud Implementation IPT and identify relevant documentation for update to address skills and occupational categories	November 30, 2022
Review skills gap analysis to determine updates to cloud strategy	May 31, 2023

ECD: November 30, 2023.

Text of Appendix IV: Comments from the U.S. Coast Guard

July 20, 2022

Jennifer R. Franks

Director, Information Technology and Cybersecurity

U.S. Government Accountability Office 441 G Street, NW

Washington, DC 20548

U.S. Department of Homeland Security

Washington, DC 20528

Re: Management Response to Draft Report GAO-22-105092, "COAST GUARD: Actions Needed to Enhance IT Program Implementation"

Dear Ms. Franks:

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

DHS leadership is pleased to note GAO's recognition that the U.S. Coast Guard incorporated most federal cloud requirements into the March 2021 Coast Guard cloud strategy and associated relevant communications and policies, including requirements relating to procurement. The Coast Guard recognizes the importance of having improved Information Technology (IT) management and Operational Technology processes and managing risks for all systems.

The draft report contained eight recommendations with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for GAO's consideration.

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

Enclosure

Enclosure: Management Response to Recommendations Contained in GAO-22-105092

GAO recommended that the Commandant of the Coast Guard direct the Deputy Commandant for Mission Support:

Recommendation 1: Develop network capacity planning policies and procedures that address the leading practices we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs.

Response: Concur. The Coast Guard’s Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Infrastructure Program is currently transitioning to the Enterprise Infrastructure Services (EIS) contract (as administered by the General Services Administration), along with additional network services that will be undertaken upon completion of the transition. Within this effort, Coast Guard’s C5I program will address the policies and procedures described within each part of this recommendation, as appropriate, given the dependency of the transition and the specific services provided by the vendor, which vary by service provider.

Actions: Estimated Completion Date (ECD)

Award of the Engineering Transition Services Contract: January 31, 2023

Award of EIS Transition Unique Contract Line Item Number: November 30, 2023

Overall Estimated Completion Date (ECD): March 29, 2024.

Recommendation 2: Implement the leading practices for network capacity planning that we identified, including (1) compiling a complete and accurate inventory of hardware, software, and configurations; (2) identifying traffic growth predictions; (3) prioritizing network traffic; (4) performing simulations and what-if-analyses; and (5) continually monitoring the health of the infrastructure to ensure it is meeting demand and mission needs.

Response: Concur. The Coast Guard C5I Infrastructure Program will implement the leading practices for network capacity planning recommended by GAO through its pending EIS contract, and will take measures to implement network capacity planning. Implementation details identified during procedure development will be used to guide the implementation. Currently, C5I is engaging an infrastructure managed service provider, which, once awarded in 2023, will provide the necessary contract vehicle for executing a proactive network capacity planning strategy.

ECD: March 29, 2024.

Recommendation 3: Establish a comprehensive and accurate inventory of all operational technology, including ICS [industrial control system] and SCADA [supervisory control and data acquisition] systems.

Response: Concur. Inventories of the Coast Guard's operational technology (i.e., devices that interact with the physical environment) are already tracked under the separate divisions who hold responsibility for the systems such as the: (1) the Surface Forces Logistics Center for Engineering Command and Control; (2) Office of Naval Engineering for fire control/weapons systems; or (3) Aviation Logistics Command for aviation control systems. The Coast Guard's Office of C5I Program Management will coordinate with stakeholders to establish a single consolidated inventory of all operational technology, including ICS and SCADA systems.

ECD: May 31, 2023.

Recommendation 4: Develop a plan or strategy for aligning all operational technology to the Department of Defense [DoD] risk management framework, including time frames for completing the alignment.

Response: Concur. The Coast Guard's Office of Information Management (CG-61) will develop a standard to ensure that operational technology is securely configured in accordance with applicable DoD policies and security controls. Once complete, this standard will set expectations for operational technology to undergo special assessment of their functional and security-related capabilities and deficiencies.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-82 Rev. 3 (Draft), “Guide to Operational Technology (OT) Security,” dated April 26, 2022: (1) expands the scope of guidance from industrial control systems to include OT; and (2) updates OT threats and vulnerabilities, risk management, recommended practices and architectures.

Within one year of the document’s completion, CG-61 will review the final version of NIST SP 800-82 to determine how to best align a future OT Cybersecurity Risk Management Implementation Standard to this guidance.

ECD: To be determined (TBD).

Recommendation 5: Ensure that the plan or strategy for aligning all operational technology to the Department of Defense Risk Management Framework is effectively implemented.

Response: Concur. The Coast Guard’s Office of Cybersecurity Program Management (CG-62) will update COMDTINST M5500.13, U. S. Coast Guard Cybersecurity Policy, to require that all OT comply with the Department of Defense risk management framework. The estimated completion date for the update the next revision of this policy is June 30, 2023.

Further, as within one year of issuance of the final update of NIST SP 800-82, which expands the scope of guidance from industrial control systems to include OT and update OT threats and vulnerabilities, risk management, recommended practices and architectures, CG-62 will also review this document and determine how to best align a future OT Cybersecurity Risk

Management Implementation Standard to this guidance and measure the effectiveness of the implementation.

ECD: TBD.

Recommendation 6: Update existing policies and procedures to explicitly describe a cybersecurity risk management process for ICS [industrial control system] and SCADA [supervisory control and data acquisition] systems.

Response: Concur. The Coast Guard’s CG-62 will ensure that the next update to the COMDTINST M5500.13 includes requirements for ICS and SCADA, as well as the importance of tracking the cybersecurity risk management of ICS and SCADA systems. Further, CG-62 will also review the updated NIST SP 800-82, within one year of completion, to determine how to best align a future OT Cybersecurity Risk Management Implementation Standard to this guidance.

ECD: TBD.

Recommendation7: Send its list of cloud services that do not meet FedRAMP [Federal Risk and Authorization Management Program] requirements to the appropriate agency head for submission to the Federal CIO [Chief Information Officer].

Response: Concur. The Coast Guard, which operates on and requires connection to the DOD Information Network, currently requires that cloud providers be in compliance with the DoD Cloud Computing Security Requirements Guide. This compliance is measured as “DoD Impact Levels,” and are the standards by which Coast Guard cloud services are procured. As these standards do not directly line up with FedRAMP, the Coast Guard’s Office of Enterprise Architecture and Technology Innovation (CG-67) will conduct a compliance review to address the action in this recommendation.

ECD: May 31, 2023.

Recommendation 8: Update the service’s cloud strategy and other relevant documentation to include a cross-walk of new and old skills and occupational categories, and to conduct a skills gap analysis.

Response: Concur. The Coast Guard will conduct a Service-wide effort, rather than a formal skills gap-analysis specific to the IT community, as part of the Commandant’s Ready Workforce 2030 efforts. Specifically, C5I will field a Cloud Implementation Integrated Product Team (IPT) to address this recommendation.

Actions	ECD
Charter Cloud Implementation IPT and identify relevant documentation for update to address skills and occupational categories	November 30, 2022
Review skills gap analysis to determine updates to cloud strategy	May 31, 2023

ECD: November 30, 2023.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Nicole Jarvis (assistant director), Di'Mond Spencer (analyst-in-charge), Brottie Barlow, Christopher Businsky, Donna Epler, William Hutchinson, Fatima Jahan, Anh Le, Ahsan Nasar, Walter Vance, and Adam Vodraska made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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