



September 2022

# COAST GUARD

## Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands

# GAO Highlights

Highlights of [GAO-22-105208](#), a report to congressional committees

## Why GAO Did This Study

The Coast Guard, a multi-mission, maritime military service within the Department of Homeland Security (DHS), is responsible for ensuring the safety and security of the nation's maritime transportation system and maritime borders. It established cyberspace as an operational domain in 2015 to help protect the marine transportation system from threats. Such threats could be delivered through the internet, telecommunications networks, and computer systems.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 includes a provision for GAO to review issues related to the Coast Guard's cyberspace workforce. This report addresses the extent the Coast Guard has (1) identified its cyberspace workforce and determined its associated mission needs and (2) implemented selected leading practices in its cyberspace workforce recruitment, retention, and training. We selected the leading practices by reviewing those identified in relevant GAO reports and federal guidance. GAO analyzed Coast Guard documentation and data and interviewed cognizant Coast Guard officials.

## What GAO Recommends

GAO is making six recommendations to the Coast Guard including to determine the cyberspace staff needed to meet its mission demands and fully implement five recruitment and retention leading practices, such as establishing a strategic workforce plan for its cyberspace workforce. DHS concurred with these recommendations.

View [GAO-22-105208](#). For more information, contact Heather MacLeod at (202) 512-8777 or [macleodh@gao.gov](mailto:macleodh@gao.gov) or David Hinchman at (214) 777-5719 or [hinchmand@gao.gov](mailto:hinchmand@gao.gov).

September 2022

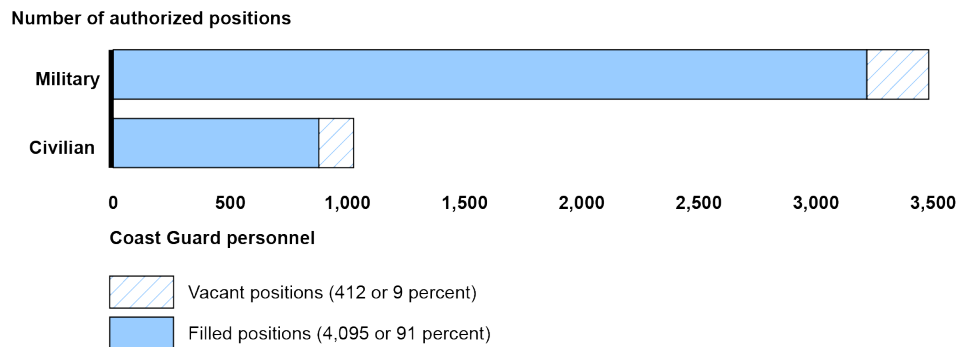
## COAST GUARD

### Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands

## What GAO Found

The Coast Guard is increasingly dependent upon its cyberspace workforce to maintain and protect its information systems and data from threats. As of September 2021, the Coast Guard determined it had 4,507 authorized cyberspace workforce positions (i.e., funded positions that could be vacant or filled), consisting of military and civilian personnel.

Authorized Coast Guard Cyberspace Positions, Filled and Vacant, as of September 2021



Source: GAO analysis of Coast Guard data. | GAO-22-105208

Coast Guard guidance calls for the service to use its Manpower Requirements Determination process to assess and determine necessary staffing levels and skills to meet mission needs. However, GAO found that the service had not used this process for a large portion of its cyberspace workforce. For example, as of February 2022, the Coast Guard had not used this process for three headquarters units that collectively represent 55 percent of its cyberspace workforce positions. Until such analysis is completed, the Coast Guard will not fully understand the resources it requires, including those to protect its information systems and data from threats.

Of 12 selected recruitment, retention, and training leading practices, the Coast Guard fully implemented seven, partially implemented three, and did not implement two. By fully implementing these leading practices, the Coast Guard could better manage its cyberspace workforce. For example, it has not developed a strategic workforce plan for its cyberspace workforce. According to leading recruitment practices, such a plan should include three elements: (1) strategic direction, (2) supply, demand, and gap analyses, and (3) solution implementation, along with monitoring the plan's progress to address all cyberspace competency and staffing needs. Without having such a plan, the Coast Guard will likely miss opportunities to recruit for difficult to fill cyberspace positions.

---

# Contents

---

Letter		1
	Background	5
	Current Cyberspace Positions Identified, but Staffing Levels to Meet Mission Needs Not Determined	8
	Most Workforce Leading Practices Are Fully or Partially Implemented, but Some Actions Needed	17
	Conclusions	27
	Recommendations for Executive Actions	27
	Agency Comments and Our Evaluation	28
Appendix I	Comments from the Department of Homeland Security	30
Appendix II	GAO Contacts and Staff Acknowledgments	34
Tables		
	Table 1: Assessment of the Coast Guard's Implementation of Five Selected Recruitment Leading Practices for Its Cyberspace Workforce	19
	Table 2: Assessment of the Coast Guard's Implementation of Three Selected Retention Leading Practices for Its Cyberspace Workforce	23
	Table 3: Assessment of the Coast Guard's Implementation of Four Selected Training Leading Practices for its Cyberspace Workforce	26
Figures		
	Figure 1: Coast Guard Authorized Cyberspace Position Categories, as of September 2021	10
	Figure 2: Number of Authorized Coast Guard Cyberspace Positions, Filled and Vacant, as of September 2021	11
	Figure 3: Coast Guard's Vacancy Gap, the Difference between Authorized and Filled Positions, in Its Civilian IT Management Series, April 2017 through February 2022	12
	Figure 4: Distribution of Cyberspace Authorized Positions across Coast Guard Units as of September 2021	15

---

Figure 5: Extent Coast Guard Has Implemented Selected  
Recruitment, Retention, and Training Leading Practices  
for Its Cyberspace Workforce

18

---

---

### Abbreviations

C5I	Command, Control, Communications, Computers, Cyber, and Intelligence
DCWF	Department of Defense Cyberspace Workforce Framework
Defense Climate Survey	Defense Organizational Climate Survey
DHS	Department of Homeland Security
DOD	Department of Defense
IT	Information Technology
MRD	Manpower Requirements Determination
NICE	National Initiative for Cybersecurity Education
OPM	Office of Personnel Management

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



September 27, 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 is a multi-mission, maritime military service within the Department of Homeland Security (DHS) composed of approximately 55,200 military and civilian personnel. It is responsible for ensuring the safety and security of the nation’s maritime transportation system and maritime borders. In 2015, the Coast Guard established cyberspace as an operational domain in its efforts to protect the U.S. marine transportation system from threats delivered in and through cyberspace. It considers cyberspace to include the internet, telecommunications networks, and computer systems.<sup>1</sup>

Like other federal agencies, the Coast Guard is increasingly dependent upon its cyberspace workforce to maintain and protect its information systems and data from threats.<sup>2</sup> In recent years, its networks and information have been exploited and maritime critical infrastructure have experienced cyberattacks. For example, according to the Coast Guard, over 500 cyberattacks occurred within the marine transportation system in 2020. It estimated that the cost of a data breach in general was about

---

<sup>1</sup>According to the Coast Guard, the cyberspace domain is the operational domain within the information environment consisting of the interdependent networks of IT, infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, processors and controllers that operate in the light spectrum—and their use in operational activities and programs.

<sup>2</sup>For the purposes of this report, we use the term “cyberspace workforce” to refer to all IT and cybersecurity personnel.

---

\$3.9 million, on average.<sup>3</sup> These events have reinforced the importance of the Coast Guard's cyber capabilities and the workforce who operate and maintain them.

The William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 includes a provision for us to examine and report on issues related to the Coast Guard's cyberspace workforce.<sup>4</sup>

This report examines the extent the Coast Guard has (1) identified its cyberspace workforce and determined its associated mission demands and (2) implemented selected leading practices in its cyberspace workforce recruitment, retention, and training.

To address the first objective, we analyzed Coast Guard data and documentation, reviewed an applicable law and standards, and interviewed cognizant Coast Guard officials. Specifically, we analyzed Coast Guard data on its cyberspace personnel, as of September 2021—the most recent date Coast Guard officials told us data were available. To assess the reliability of the data, we (1) reviewed the Coast Guard's procedures manual for identifying and recording personnel within its cyberspace workforce, (2) performed electronic testing, such as testing for missing data, and (3) interviewed Coast Guard officials from its Office of Cyberspace Forces about their practices for maintaining the data.<sup>5</sup> We determined that the data were sufficiently reliable for the purpose of reporting characteristics of authorized cyberspace positions (funded positions available for the Coast Guard to fill). Specifically, these characteristics included the personnel type (i.e., military or civilian), status (i.e., filled or vacant), cyberspace category (e.g. Cyberspace IT or Cybersecurity), and unit type. In addition, we reviewed an applicable law and standards for identifying the cyberspace workforce and interviewed

---

<sup>3</sup>Coast Guard, *Cyber Strategic Outlook*, (Aug. 2021).

<sup>4</sup>Pub. L. No. 116-283, § 8258(a), 134 Stat. 3388, 4677-78 (2021).

<sup>5</sup>Coast Guard, *USCG Cyber Position Coding Process Guide*, (Aug. 5, 2021).

---

officials from the Coast Guard’s Office of Cyberspace Forces to understand how the service implemented them.<sup>6</sup>

We also analyzed the Coast Guard’s documentation on its process for determining workforce staffing levels needed for its cyberspace mission needs. Documentation we analyzed included the *Coast Guard’s Manpower Requirement Determination Tactics, Techniques, and Procedures* and its most recently issued *Manpower Requirements Plan*.<sup>7</sup> In addition, we reviewed documentation on the Coast Guard’s status in conducting workforce analysis—known as Manpower Requirements Analysis—for its cyberspace workforce. We compared this information against Coast Guard guidance for conducting these analyses and its human capital strategy documentation.<sup>8</sup>

To address the second objective, we first identified topic areas associated with human capital management based on our review of workforce planning and management reports we issued, as well as guidance from the Office of Personnel Management (OPM) and the Office of Management and Budget. From these topic areas, we selected five that were of particular importance to successful workforce planning: (1) strategic workforce planning, (2) recruiting and hiring efforts, (3) retention incentives, (4) employee morale, and (5) training and development. We

---

<sup>6</sup>*Federal Cybersecurity Workforce Assessment Act of 2015*, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (2015); National Institute of Standards and Technology, *NICE Framework for Improving Critical Infrastructure Cybersecurity*, (Apr. 16, 2018); Department of Defense Directive 8140.01, *Cyberspace Workforce Management* (Oct. 5, 2020).

<sup>7</sup>Coast Guard, *Coast Guard Manpower Requirement Determination Tactics, Techniques, and Procedures*, (Apr. 2021). Coast Guard, *Manpower Requirements Plan*, (Apr. 13, 2018).

<sup>8</sup>Coast Guard, *Manpower Requirements Manual*, (Nov. 9, 2020). Coast Guard, *Human Capital Strategy*, (Jan. 2016).



---

selected 12 leading practices applicable to these topic areas.<sup>9</sup> These 12 practices can be categorized as supporting the recruitment, retention, or training of the cyberspace workforce.

We then reviewed Coast Guard documentation on its cyberspace workforce recruitment, retention, and training efforts, including policies and plans applicable to the cyberspace workforce. We compared them to the 12 leading practices we selected. We determined whether the Coast Guard had fully implemented, partially implemented, or not implemented each of the 12 selected applicable leading practices.<sup>10</sup> To supplement our

---

<sup>9</sup>We have previously found these topic areas to be of particular importance to successful workforce planning. Four of the five topic areas were previously identified as part of our high-risk and key issues work on human capital management. We added the fifth topic area (retention incentives) based on our research and consultation with our in-house human capital experts. To select these leading practices, we reviewed those identified in six of our past reports, as well as two guidance documents from OPM and the Office of Management and Budget on strategic workforce planning, recruiting and hiring efforts, retention incentives, employee morale, and training and development. See *Federal Workforce: Key Talent Management Strategies for Agencies to Better Meet Their Missions*, [GAO-19-181](#) (Washington, D.C.: Mar. 28, 2019); *U.S. Secret Service: Action Needed to Address Gaps in IT Workforce Planning and Management Practices*, [GAO-19-60](#) (Washington, D.C.: Nov. 15, 2018); *IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, [GAO-17-8](#) (Washington, D.C.: Nov. 30, 2016); *Human Capital: A Guide for Assessing Strategic Training and Development Efforts in the Federal Government (Supersedes GAO-03-893G)*, [GAO-04-546G](#) (Washington, D.C.: Mar. 1, 2004); *Human Capital: Additional Collaboration Between OPM and Agencies Is Key to Improved Federal Hiring*, [GAO-04-797](#) (Washington, D.C.: June 7, 2004); *A Model of Strategic Human Capital Management*, [GAO-02-373SP](#) (Washington, D.C.: Mar. 15, 2002); Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (July 12, 2016); Office of Management and Budget and OPM, *Institutionalizing Hiring Excellence to Achieve Mission Outcomes*, M-17-03 (Nov. 1, 2016).

<sup>10</sup>We considered *fully implemented* where we found information obtained from Coast Guard documentation and interviews demonstrated all aspects of the applicable leading practice. We considered *partially implemented* where we found information obtained from Coast Guard documentation and interviews demonstrated some, but not all, aspects of the applicable leading practice. We considered *not implemented* where we found Coast Guard officials did not provide any documentation, or if they provided documentation or information from interviews, it did not demonstrate any aspect of the applicable leading practice.

---

analysis, we interviewed officials from Coast Guard offices and commands with key cyberspace responsibilities.<sup>11</sup>

We also analyzed Coast Guard data on recruitment and retention incentives the service provided to its cyberspace workforce from fiscal years 2019 through 2021. The Coast Guard did not have retention incentive data available on civilian and officer personnel for fiscal year 2019, because it had not provided incentives to the cyberspace workforce during this time. To assess the reliability of the data, we reviewed the Coast Guard's guidance for providing these incentives and interviewed officials about their practices for maintaining the data.<sup>12</sup> We determined that the data were sufficiently reliable for the purpose of reporting the number of personnel who received these incentives and the amount provided.

We conducted this performance audit from May 2021 to September 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.

---

## Background

---

### Coast Guard Cyberspace Workforce

The Coast Guard defines its cyberspace workforce as all personnel who design, build, configure, operate, maintain, defend, protect, and preserve Coast Guard cyber resources, conduct cyber-related intelligence activities, and enable current and future cyber operations.<sup>13</sup> As part of the cyberspace workforce, personnel maintain IT by acquiring, implementing, evaluating, and disposing of computers, software, and related resources.

---

<sup>11</sup>We interviewed officials from the following Coast Guard offices and commands: Cyberspace Forces, Workforce Forecasting and Analysis, Civilian Human Resources Operations, Civilian Workforce Management, Force Readiness Command, Coast Guard Recruiting Command, and Deputy Commandant for Mission Support-Deputy for Personnel Readiness.

<sup>12</sup>We interviewed officials from the Coast Guard's Office of Workforce Forecasting and Analysis, and Office of Civilian Human Resources Operations.

<sup>13</sup>Coast Guard, *United States Coast Guard Cyber Strategic Outlook*, (Aug. 2021).

---

The Coast Guard cyberspace workforce consists of both military and civilian personnel.<sup>14</sup> Its military workforce consists of enlisted and officer personnel.<sup>15</sup>

- **Enlisted personnel.** These personnel obtain a rating, which is a general occupation category requiring specific skills and abilities. For example, the Coast Guard categorizes personnel in its Information Systems Technician rating and the Electronics Technician rating as part of the cyberspace workforce. Personnel in the Information Systems Technician rating maintain, repair, or install computer and telephone equipment across the Coast Guard organization. Personnel in the Electronics Technician rating install, maintain, repair, or manage electronic equipment, including data and voice-encryption equipment. The Coast Guard also categorizes personnel who perform cyberspace duties from five additional ratings as part of the cyberspace workforce.<sup>16</sup>
- **Officer personnel.** These personnel obtain a specialty code, which is an identification of their area of expertise and required competencies, education, training, and certifications. For example, personnel with the cyberspace officer specialty code are trained, cleared, and qualified to build, secure, operate, defend, and protect Coast Guard and national cyberspace resources.
- **Civilian personnel.** This workforce consists of non-military personnel that OPM classifies into an occupational series, which is a grouping of positions with a similar line of work and qualification requirements. For example, the Coast Guard's civilian IT Management series covers positions that manage, supervise, lead, administer, develop, deliver, and support IT systems and services.

---

<sup>14</sup>As of April 2022, the Coast Guard stated that it had a total workforce of 55,236—including 46,235 military and 9,001 civilian personnel.

<sup>15</sup>Active-duty personnel are full-time enlisted and officer personnel responsible for carrying out the Coast Guard's missions. The military workforce also includes reserve personnel. These are part-time enlisted and officer personnel. They are trained and qualified to take duty in times of war or national emergency and to augment Coast Guard forces and provide surge capacity to respond to natural or human-made disasters, accidents, and all other hazards.

<sup>16</sup>These five other ratings are: (1) Avionics Electrical Technician, (2) Boatswain's Mate, (3) Intelligence Specialist, (4) Operations Specialist, and (5) Marine Science Technician.

---

## Coast Guard's New and Reorganized Cyberspace Entities

In recent years, the Coast Guard has established and reorganized its headquarters cyberspace entities. In 2017, it created an Office of Cyberspace Forces to manage the cyberspace workforce. In 2020, the Coast Guard reorganized several units to establish a new 800 personnel Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Service Center to manage C5I product lines and support its systems, among other responsibilities. In 2022, it established a new cyber protection team consisting of 44 personnel to focus on cybersecurity at critical ports of entry.<sup>17</sup>

---

## Federal Cyberspace Workforce Challenges and Initiatives

A resilient, well-trained, and dedicated cyberspace workforce is essential to protecting federal IT systems. Nevertheless, the Office of Management and Budget and our prior reports have pointed out that the federal government faces a persistent shortage of cybersecurity and IT professionals to implement and oversee information security protections to combat cyber threats.<sup>18</sup>

We have reported that effective workforce planning is key to addressing the federal government's IT challenges and ensuring that agencies have staff with the necessary knowledge, skills, and abilities to execute a range of management functions that support agencies' missions and goals.<sup>19</sup> Further, we have noted that effectively implementing workforce planning activities can facilitate the success of major IT acquisitions. To this end, in November 2016, we issued an IT workforce planning framework that identifies four steps and eight activities, including assessing gaps in competencies and skills, and developing strategies and plans to address them.<sup>20</sup>

In recent years, the federal government has taken various steps to improve its cybersecurity workforce. These include the National Institute

---

<sup>17</sup>The Coast Guard has two other cyber protection teams. According to the Coast Guard's *Fiscal Year 2022-2023 Strategic Planning Direction*, the teams are a deployable force that protect critical Coast Guard networks and the maritime transportation system.

<sup>18</sup>*High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021).

<sup>19</sup>*Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities*, [GAO-20-129](#) (Washington, D.C.: Oct. 30, 2019). As mentioned previously, the Coast Guard's cyberspace workforce includes its IT workforce.

<sup>20</sup>*IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps*, [GAO-17-8](#) (Washington, D.C.: Nov. 30, 2016).

---

of Standards and Technology coordinating the National Initiative for Cybersecurity Education (NICE) to promote cybersecurity training and skills, and OPM developing guidance to address cybersecurity workforce challenges.<sup>21</sup> NICE also developed the *National Cybersecurity Workforce Framework (NICE framework)*, which is intended to provide a consistent way to define and describe cybersecurity work at any public or private organization, including federal agencies.<sup>22</sup>

In addition, the *Federal Cybersecurity Workforce Assessment Act of 2015* requires federal agencies to identify and assign an employment code to all positions that require the performance of cybersecurity or other cyber-related functions.<sup>23</sup> According to the Act, federal agencies are to assign this code in alignment with the *NICE framework*. The Act also requires all federal agencies to identify and report to OPM on its cyberspace work roles of critical need and submit an annual progress report to Congress.

---

## Current Cyberspace Positions Identified, but Staffing Levels to Meet Mission Needs Not Determined

---

### Cyberspace Positions Identified

As of September 2021, the Coast Guard determined it had 4,507 authorized cyberspace workforce positions—7.6 percent of its approximately 59,300 total authorized positions (i.e., funded positions that may be vacant or filled). According to our analysis of Coast Guard data, 77 percent of the authorized cyberspace positions were military and 23 percent were civilian. In 2018, the Coast Guard completed identifying all cyberspace positions and assigning employment codes to them, in accordance with the *Federal Cybersecurity Workforce Assessment Act of*

---

<sup>21</sup>Office of Personnel and Management, *The Guide to Data Standards* (Washington, D.C.: Nov. 15, 2014).

<sup>22</sup>National Institute of Standards and Technology, *NICE Cybersecurity Workforce Framework*, Special Publication 800-181 (Gaithersburg, Md.: Aug. 2017).

<sup>23</sup>Pub. L. No. 114-113, §303, 129 Stat. 2242, 2975-76. The requirement for DHS to collect and report this information ends in fiscal year 2022. Pub. L. No. 114-113, §304(a), 129 Stat. 2242, 2977. See *generally* Federal Cybersecurity Workforce Assessment Act of 2015, Pub. L. No. 114-113, Div. N, Title III, 129 Stat. 2242, 2975-77 (2015).

---

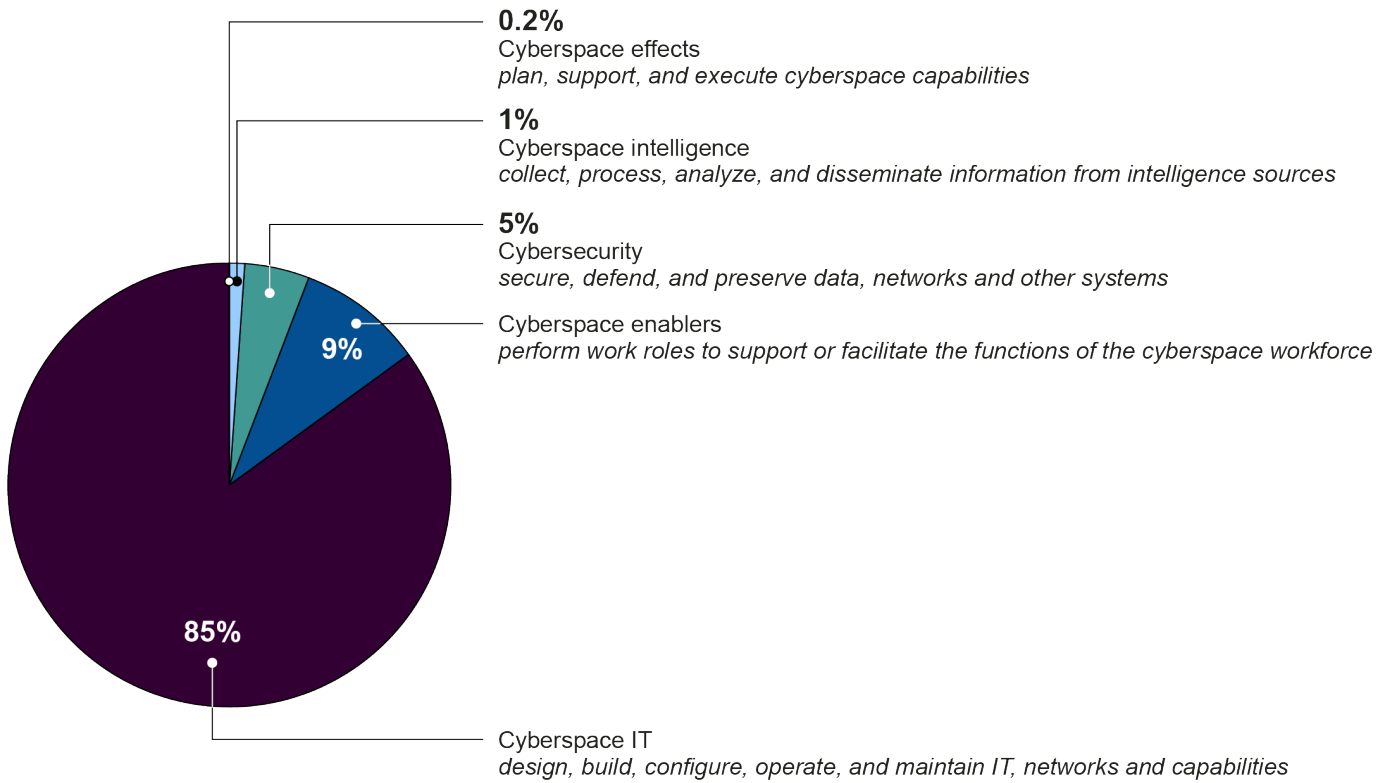
2015, NICE framework, and Department of Defense (DOD) cybersecurity standards.<sup>24</sup>

The Coast Guard's authorized cyberspace positions consist of personnel in five categories: (1) Cyberspace IT, (2) Cyberspace Enablers, (3) Cybersecurity, (4) Cyberspace Intelligence, and (5) Cyberspace Effects. According to our analysis of Coast Guard data, positions in the Cyberspace IT category made up 85 percent of the service's identified authorized cyberspace positions (see figure 1), as of September 2021, the most recent data available.

---

<sup>24</sup>A 2017 memorandum of agreement between the Department of Defense (DOD) and DHS established that the Coast Guard would adhere to DOD cybersecurity standards, requirements, and policies. According to Coast Guard guidance, the Coast Guard used the DOD Cyberspace Workforce Framework (DCWF) as the authoritative reference for its identification, tracking, and reporting of its cyberspace positions. The DCWF aligns to the NICE framework. The DCWF categorizes cyberspace positions using a three-digit employment code. For example, the DCWF code "451" identifies a System Administrator who installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts. See Coast Guard, *USCG Cyber Position Coding Process Guide* (Aug. 5, 2021).

**Figure 1: Coast Guard Authorized Cyberspace Position Categories, as of September 2021**



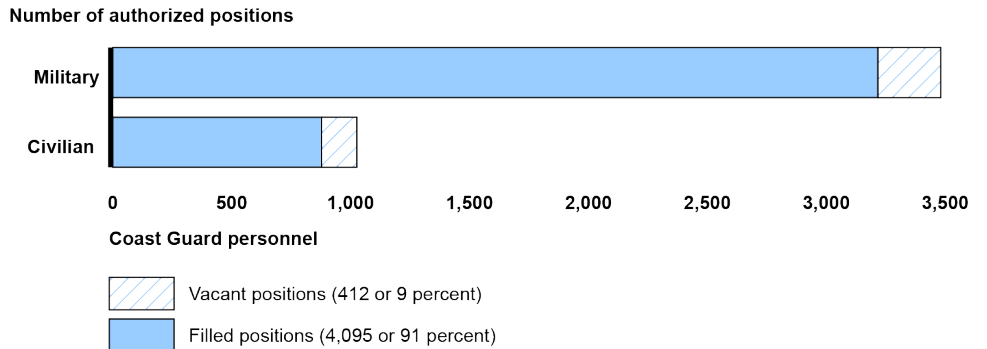
Source: GAO analysis of Coast Guard data. | GAO-22-105208

Note: Authorized positions are those that are funded and may be vacant or filled.

Additionally, Coast Guard data showed the service’s civilian cyberspace workforce had a greater share of vacancies than its military cyberspace workforce. As of September 2021, 412 (9 percent) of the Coast Guard’s total authorized cyberspace workforce positions were vacant (see fig. 2).<sup>25</sup> This included 148 vacancies (14 percent) among its 1,026 authorized civilian cyberspace workforce positions and 264 vacancies (8 percent) among its 3,481 military cyberspace workforce positions.

<sup>25</sup>For context, according to our analysis of Coast Guard data, the Coast Guard’s overall civilian vacancy rate is 15.5 percent as of February 2022; the officer vacancy rate is 10.2 percent, and the enlisted vacancy rate is 3.6 percent as of March 2022.

**Figure 2: Number of Authorized Coast Guard Cyberspace Positions, Filled and Vacant, as of September 2021**



Source: GAO analysis of Coast Guard data. | GAO-22-105208

According to Coast Guard documentation, the service has faced persistent challenges filling certain cyberspace positions it considers as critical, or understaffed. For example, on the military workforce side, it had 75 vacancies in its Electronics Technician enlisted rating, as of September 2021. Positions in this rating make up approximately half (1,251) of the 2,661 enlisted cyberspace workforce positions. According to an October 2021 memo, the Coast Guard identified filling positions for this rating as critical and offered a recruitment bonus for it. We discuss the Coast Guard’s recruitment, retention, and training efforts in more detail later in this report.

On the civilian workforce side, the Coast Guard has faced particular challenges in filling positions within its civilian IT Management series, its largest civilian cyberspace workforce position category.<sup>26</sup> Specifically, the IT management series accounts for 58 percent of the civilian cyberspace authorized positions. According to an April 2021 Coast Guard memo, the service has had difficulty filling and retaining personnel for these positions because many were leaving for higher paying positions in the private sector.<sup>27</sup> The memo states that retaining these personnel is mandatory for remaining resilient to cyber threats.

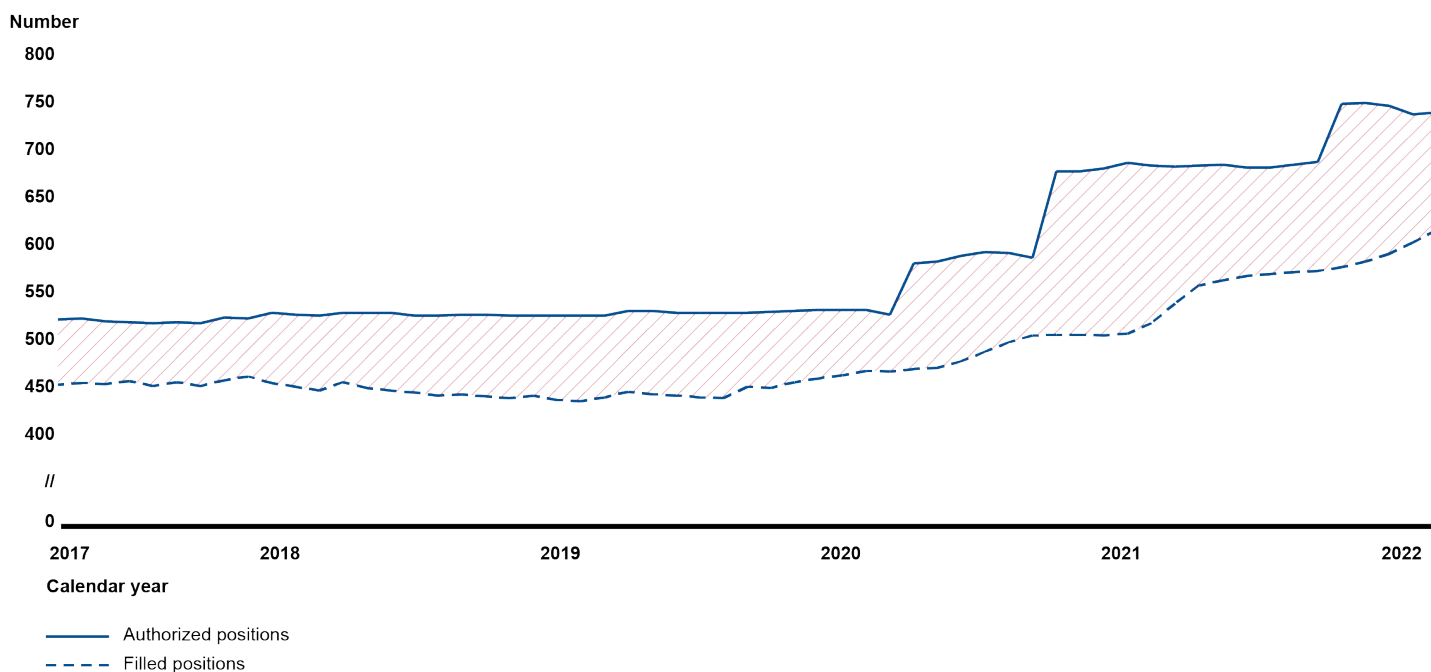
<sup>26</sup>Such personnel are responsible for managing and developing IT systems and services.

<sup>27</sup>Coast Guard, *FY22 Workforce Planning Team (WPT) Intervention Requests for Civilian Cyberspace Workforce*, (Apr. 5, 2021).



From April 2017 through February 2022, the Coast Guard consistently had a vacancy gap (i.e., the difference between authorized and filled positions) of civilian IT Management positions. Specifically, this gap ranged from a low of 51 positions in March 2020 to a high of 188 positions in January 2021. This is because the Coast Guard considerably increased its authorized positions in its civilian IT Management series between March 2020 and February 2022. Notably, during this time, the Coast Guard increased these authorized positions from 523 to 736—a 41 percent increase. Figure 3 shows that while the Coast Guard has filled these positions at a greater rate, its gap between the number of authorized and filled positions has remained.

**Figure 3: Coast Guard’s Vacancy Gap, the Difference between Authorized and Filled Positions, in Its Civilian IT Management Series, April 2017 through February 2022**



Source: GAO analysis of Coast Guard data. | GAO-22-105208

### Staffing Levels Needed to Meet Cyberspace Mission Demands Have Not Been Determined

The Coast Guard has undertaken several efforts to plan and manage its workforce, but has not determined the cyberspace workforce staffing levels needed to meet its growing mission demands. While the Coast Guard has determined the number of authorized cyberspace positions, or funded positions available for it to fill, it has not determined the number of

---

positions and necessary mix of skills to meet mission demands—which could be higher or lower than the number of authorized positions.

In response to increased cyber mission-related demands, the Coast Guard established multiple new cyberspace entities and the authorized positions to support them. For example, in 2013, the Coast Guard established the Cyber Command, and in 2015, it established cyberspace as a new operational domain. It subsequently established new cyber-focused entities and the positions to support them. For example, in 2020, it established the C5I Service Center within its Office of Information Technology.

According to the Coast Guard’s Manpower Requirements Determination (MRD) guidance, new components or cross-sections of the organization should be assessed to determine appropriate staffing levels. Specifically, the Coast Guard’s Manpower Requirements Manual states that MRDs provide a means to understand the effect on the workforce of existing, new, or modified missions or business processes. The MRD process starts with an analysis—referred to as a Manpower Requirements Analysis—that defines both the number of workers and the necessary mix of skills for the positions required. The MRD uses results from this analysis to identify the number and type of positions a unit (i.e., organized groups of Coast Guard personnel with a similar purpose) requires to meet mission-based capability requirements.

In February 2020, we found the Coast Guard had used this process to assess and determine a small portion of its total workforce needs—and recommended, among other things, the service plan for how it will meet its goal of using the process to assess its service-wide workforce needs.<sup>28</sup> The Coast Guard concurred and reported it would update its Manpower Requirements Plan with the information. As of June 2022, the Coast Guard stated plans to do so by the end of calendar year 2022.

The Coast Guard is increasingly dependent upon its cyberspace workforce to maintain and protect its information systems and data from threats. This makes it crucial for the service to understand the necessary

---

<sup>28</sup>Specifically, we recommended that the service update its April 2018 Manpower Requirements Plan to include time frames and milestones for completing manpower requirements analyses and determinations for all positions and units. *Coast Guard: Actions Needed to Evaluate the Effectiveness of Organizational Changes and Determine Workforce Needs*, [GAO-20-223](#) (Washington, D.C.: Feb. 26, 2020).

---

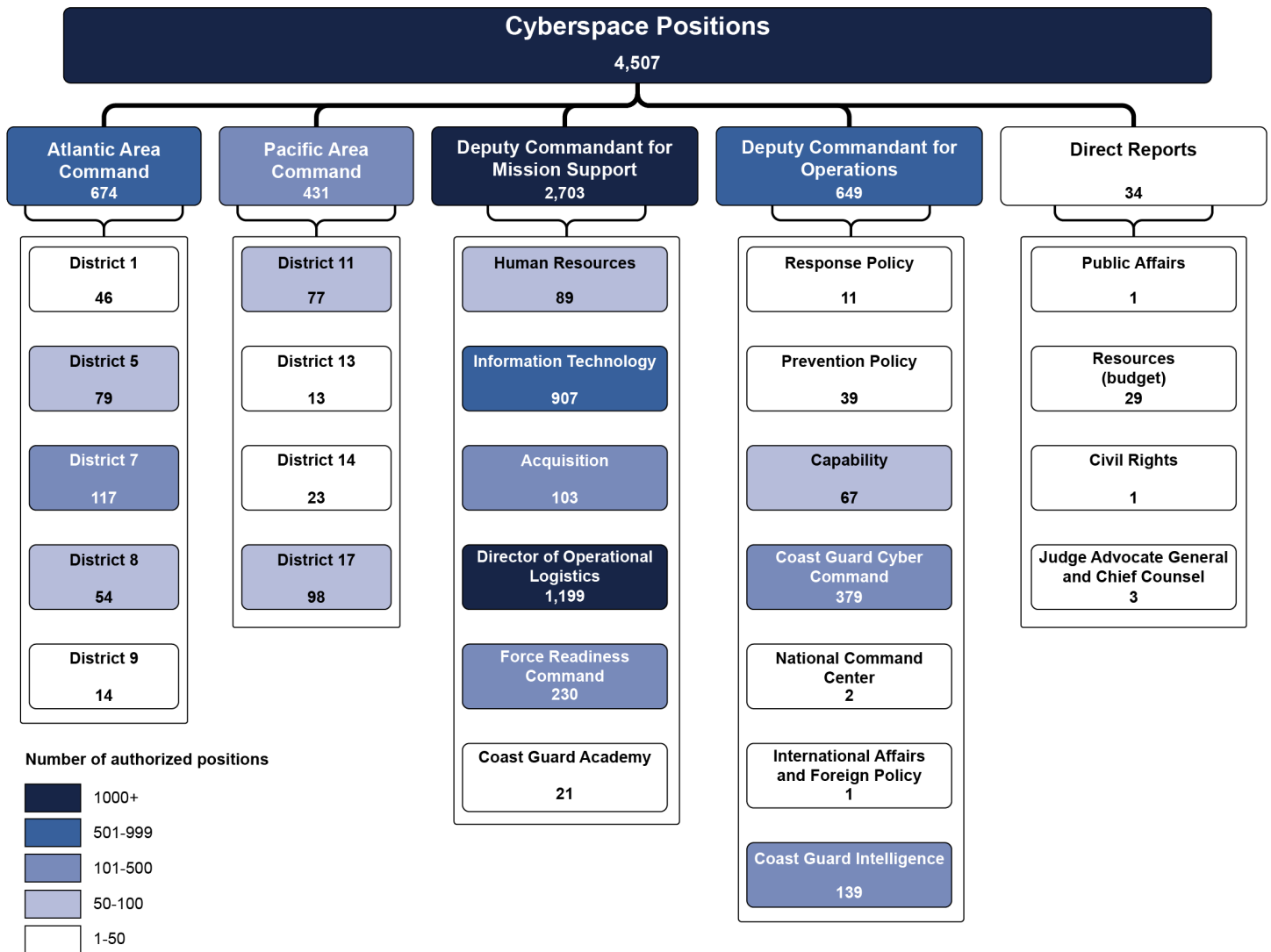
cyberspace workforce staffing levels it requires to fulfill its mission demands.

However, the Coast Guard has not used the MRD process to assess and determine necessary workforce levels and skills for large portions of its cyberspace workforce units. This includes three headquarters units that represent 55 percent of its cyberspace workforce positions—Cyber Command, Office of Information Technology, and Office of the Director of Operational Logistics.<sup>29</sup> As of February 2022, the Coast Guard had not used its MRD process to determine its cyberspace workforce needs for these units. Moreover, the cyberspace workforce spans at least 20 additional units. Figure 4 shows the distribution of Coast Guard cyberspace authorized positions across its various units.

---

<sup>29</sup>In April 2022, the Coast Guard approved funding to conduct an MRD on its Cyber Command. According to Coast Guard officials, the MRD process will begin in September 2022 and will take approximately one year to complete.

Figure 4: Distribution of Cyberspace Authorized Positions across Coast Guard Units as of September 2021



Source: GAO analysis of Coast Guard data. | GAO-22-105208

Note: Figure 4 is based on the Coast Guard's official organizational chart. The columns do not add up to the total number of cyberspace positions, because we did not include positions within smaller units (i.e., organized groups of Coast Guard personnel with a similar purpose), such as cutters. Moreover, the Coast Guard did not specify the units in which some positions belonged. The Information Technology unit is known as the Assistant Commandant for Command, Control, Communications, Computer, and IT.

The Coast Guard's field structure is organized under two area commands, the Atlantic and the Pacific. These two area commands oversee nine districts, which collectively oversee 37 sectors. Coast Guard headquarters is divided into two entities—its Deputy Commandant for Operations, which leads operations, and its Deputy Commandant for Mission Support, which supports them.

---

According to Coast Guard officials, the Office of Workforce Forecasting and Analysis currently focuses on tracking the number of personnel who are departing the service and works on retaining those authorized positions, rather than determining the workforce necessary to meet mission needs. However, these officials also told us they recognized the importance of assessing their cyberspace workforce needs using the MRD process, but faced challenges in doing so. Namely, Coast Guard officials said that a challenge with completing an MRD on its entire cyberspace workforce is that it is distributed across different Coast Guard units, including Cyber Command, Office of Information Technology, Director of Operational Logistics, and numerous field units with IT departments and staffs (i.e., bases, cutters, and district staffs).

Officials added that the Coast Guard's current practice is to use the MRD process at the unit level rather than the entire workforce level due to limited resources. They noted that, as resources permit, the Coast Guard would continue to conduct this process across its units. For example, they explained that in September 2022 the Coast Guard would begin using the MRD process to assess its Cyber Command. They said they planned to assess elements of the Office of Information Technology in fiscal year 2023.

According to the Coast Guard's MRD guidance, the service is to conduct an MRD when a unit's mission, function, or task requirements change. This includes when it establishes new organizational entities, proposes changes to them, or makes changes to a unit's mission capability. Moreover, the Coast Guard's *Human Capital Strategy* states that managers must define the workforce that they need to perform or support Coast Guard missions.<sup>30</sup>

In recent years, the Coast Guard's cyber-related mission demands have expanded to cover new entities and initiatives—which the service's guidance states should be assessed to determine appropriate staffing levels. By assessing and determining the staffing levels necessary to meet its growing cyberspace mission demands, the Coast Guard can better understand the resources it requires, including those to protect its information systems and data from threats.

---

<sup>30</sup>Coast Guard, *Human Capital Strategy*, (Jan. 2016).

---

---

## Most Workforce Leading Practices Are Fully or Partially Implemented, but Some Actions Needed

Among the 12 selected recruitment, retention, and training leading practices that we identified as central to effectively managing the cyberspace workforce, we found the Coast Guard fully implemented seven, partially implemented three, and did not implement two.<sup>31</sup> Specifically, the Coast Guard fully implemented all four leading practices related to training, partially implemented three related to recruitment and retention, and did not implement two related to recruitment and retention.

Figure 5 describes the 12 selected recruitment, retention, and training leading practices and the extent the Coast Guard has implemented them for its cyberspace workforce.

---

<sup>31</sup>We selected 12 leading practices that were of particular relevance to successful workforce planning and management by reviewing Office of Management and Budget and OPM federal guidance and our prior work. For example, see Office of Management and Budget, *Federal Cybersecurity Workforce Strategy*, Memorandum M-16-15 (July 12, 2016); Office of Management and Budget; and OPM, *Institutionalizing Hiring Excellence to Achieve Mission Outcomes*, M-17-03 (Nov.1, 2016).

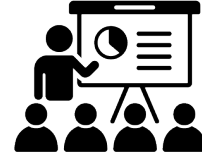
**Figure 5: Extent Coast Guard Has Implemented Selected Recruitment, Retention, and Training Leading Practices for Its Cyberspace Workforce**



**Recruitment**



**Retention**



**Training**



Fully implemented    
 Partially implemented    
 Not implemented

Source: GAO analysis of Coast Guard data. | GAO-22-105208

Fully implemented = Coast Guard information demonstrated all aspects of the applicable leading practice.  
 Partially implemented = Coast Guard information demonstrated some, but not all, aspects of the applicable leading practice.  
 Not implemented = Coast Guard information did not demonstrate any aspects of the applicable leading practice.

**Recruitment: Three of Five Selected Leading Practices Are Partially or Not Implemented**

Of the five selected recruitment leading practices, the Coast Guard fully implemented two, partially implemented two, and did not implement one for its cyberspace workforce. Table 1 summarizes our assessment of the Coast Guard’s implementation of each of the five selected recruitment leading practices.

**Table 1: Assessment of the Coast Guard’s Implementation of Five Selected Recruitment Leading Practices for Its Cyberspace Workforce**

Selected Recruitment Leading Practice	Assessment	Explanation
1. Establish and maintain a strategic workforce planning process, including developing strategies and implementing activities to address all competency and staffing needs.	○	The Coast Guard did not have a complete strategic process or plan for its cyberspace workforce that contained essential elements, such as a (1) strategic direction, (2) supply, demand, or gap analysis and (3) solution implementation, along with implementing activities to address all cyberspace competency and staffing needs. While the Coast Guard has a <i>Human Capital Strategy</i> and a <i>Cyber Strategic Outlook</i> , these documents did not contain those elements.
2. Use data to inform workforce planning and strategic recruitment.	◐	The Coast Guard used data to inform its workforce planning and recruitment for some, but not all of its cyberspace workforce. On the civilian side, it did so for positions within its civilian IT Management series, which it identified as having vacant positions. <sup>a</sup> However, on the military side, while it had data on its officers to inform its planning, it did not have data for its enlisted cyberspace personnel.
3. Recruit continuously and start the hiring process early in the school year.	●	The Coast Guard’s process includes recruiting all military and civilian personnel, including cyberspace personnel, throughout the school year. To recruit military personnel, the Coast Guard administers a continuous and comprehensive year-round recruitment cycle that includes 42 boot camps and eight officer training courses. The Coast Guard’s Recruiting Command also holds 12 officer selection panels per year. To recruit civilian personnel, the Coast Guard participated in recruitment fairs in fiscal years 2016 through 2020.
4. Leverage available hiring flexibilities such as recruitment bonuses, relocation expenses, and student loan repayments.	●	The Coast Guard leveraged hiring flexibilities such as recruitment incentives for its military and civilian cyberspace personnel. For example, according to our analysis of Coast Guard data, in fiscal year 2021, the Coast Guard provided \$440,000 to 22 military personnel as a recruitment bonus and \$615,579 to 59 civilian cyberspace personnel, among other hiring flexibilities.



Selected Recruitment Leading Practice	Assessment	Explanation
5. Establish and track metrics to monitor the effectiveness of the recruitment program and hiring process, including their effectiveness at addressing skill and staffing gaps, and report to agency leadership on progress addressing those gaps.	●	The Coast Guard established and tracked metrics, including staffing gaps or targets, for some but not all of its cyberspace workforce. It did so on the military side for its officer workforce and for part of the civilian workforce. However, it had not developed metrics for all the civilian or the enlisted cyberspace workforce. Additionally, of the metrics established, the service had not always used them to monitor the effectiveness of its recruiting and hiring of cyberspace personnel nor always reported the progress to leadership.

- Fully implemented = Coast Guard information demonstrated all aspects of the applicable leading practice.
- Partially implemented = Coast Guard information demonstrated some, but not all, aspects of the applicable leading practice.
- Not implemented = Coast Guard information did not demonstrate any aspects of the applicable leading practice.

Source: GAO analysis of Coast Guard data and documentation. | GAO-22-105208.

<sup>3</sup>According to an April 2021 Coast Guard memorandum on the intervention requests for the civilian cyberspace workforce, the Coast Guard used data on the percentage of vacant positions within its civilian IT Management series for workforce planning efforts.

### Strategic workforce planning process

In June 2022, Coast Guard officials from the Office of Cyberspace Forces stated that they were developing a management plan to govern the Coast Guard’s cyberspace workforce. They told us that they are developing this plan as part of the implementation of a new Cyber Mission Specialist rating, which we discuss in the next section. Coast Guard officials told us they anticipate completing the plan by calendar year 2024.<sup>32</sup> However, officials did not provide documentation on the status of their efforts. Without a strategic workforce plan that includes strategies and implementing activities to address all cyberspace competency and staffing needs, the Coast Guard will likely miss opportunities to recruit for difficult-to-fill cyberspace positions.

### Workforce planning and strategic recruitment data

The Coast Guard has used data to inform its workforce planning for its civilian IT Management series and cyberspace officers. On the civilian side, the Coast Guard developed reports that contained data on the percent of vacant positions within the IT Management series. For example, according to these reports, from January 2021 to February 2022, the vacancy rate for these positions decreased from 26 percent to

<sup>32</sup>Coast Guard officials told us that their intention was to implement the new cyberspace rating before completing the plan.

---

Recruitment program and hiring process metrics

---

about 17 percent.<sup>33</sup> On the military side, the Coast Guard had data on its cyberspace officers. According to its fiscal year 2021 Officer Accession Plan, the Coast Guard used data to determine the short and long-term targets to meet its workforce needs for cyberspace officers. In this plan, the Coast Guard also determined short-term targets of four accessions and long-term targets of 15 accessions to meet its workforce needs.<sup>34</sup>

However, the Coast Guard does not have similar data for its enlisted cyberspace personnel, because it has not implemented a cyberspace rating for them. Having a rating, which categorizes enlisted personnel according to different skill sets, identifies enlisted personnel for the purposes of data analysis. In January 2022, the Coast Guard approved the establishment of a Cyber Mission Specialist enlisted rating and warrant officer specialty. Officials told us that they are developing a management plan as part of the implementation of this rating. Officials added that the Coast Guard would not implement the new rating until calendar year 2023 or 2024. By incorporating data from the Cyber Mission Specialist rating to inform its strategic workforce planning, the Coast Guard will be in a better position to plan and recruit its enlisted cyberspace workforce.

The Coast Guard has established and tracked metrics for its military officer accessions and part of its civilian hiring, including staffing gaps and targets, but not the entire cyberspace workforce. Of the metrics established, the service has not always monitored their effectiveness for recruiting and hiring the three categories of cyberspace personnel below:

**Officer.** In 2019, the Coast Guard established the cyberspace officer specialty code, and in fiscal year 2021, added these officers as a personnel category in its Officer Accession Plan.<sup>35</sup> According to this plan, which is reported to Coast Guard leadership, the Coast Guard has

---

<sup>33</sup>A vacancy rate is the difference between authorized and filled positions, divided by the number of authorized positions.

<sup>34</sup>An accession is the process through which an individual becomes military personnel in the Coast Guard.

<sup>35</sup>In 2019, the Coast Guard established a new officer specialty code, which is an identification of their area of expertise and required competencies, education, training, and certifications. The Coast Guard also established four sub-specialty codes that align to the segments of the cyberspace workforce: Cyberspace IT, Cybersecurity, Cyberspace Effects, and Cyber Intelligence. A cyberspace officer is one with the cyberspace officer specialty code or sub-specialty code that correspond to the cyberspace workforce categories.

---

metrics that show the long and short-term targets for filling cyberspace officer positions. These metrics show the effectiveness of recruiting, such as whether the Coast Guard fills officer targets and meets recruitment goals. Although these plans had metrics to show the effectiveness of recruiting, they did not include metrics to show the Coast Guard's effectiveness in addressing skills or staffing gaps.

**Enlisted.** In its fiscal year 2021 Enlisted Accessions Plan, which the Assistant Commandant for Human Resources reports to leadership, the Coast Guard has metrics that show planned and actual numbers of accessions for enlisted personnel. While this plan contains goals on recruiting enlisted personnel, they are not specific to cyberspace personnel.

**Civilian.** According to its April 2017 through February 2022 reports to leadership, the Coast Guard has metrics for vacancy, attrition, and hiring regarding the civilian IT Management series. Officials told us they conducted a study on this series because, as mentioned earlier, the Coast Guard has consistently fallen short of hiring its authorized positions and did not expect to fill many vacancies within this series. For example, according to Coast Guard reports, in February 2022, the vacancy rate for this series was 16.8 percent—with a total workforce of 612 filled positions out of 736 authorized positions. However, these reports do not show how these metrics helped the Coast Guard in addressing skills or staffing gaps because they only showed the vacancies within the position and not how the Coast Guard was addressing them.

Coast Guard officials told us they had not established and tracked metrics to monitor the effectiveness of the recruitment program and hiring process for their enlisted and civilian workforce for two reasons. First, Coast Guard leadership has recently approved the Cyber Mission Specialist enlisted rating. Since this rating is new, officials said, the Coast Guard has not established metrics to monitor its effectiveness on recruiting and hiring for the enlisted personnel. Second, according to Coast Guard officials from the Office of Civilian Human Resources Operations and Office of Workforce Forecasting and Analysis, within its cyberspace workforce, the Coast Guard had only conducted a study on its civilian IT Management series. Accordingly, it does not have the metrics to monitor its effectiveness on recruiting and hiring for other series.

The Coast Guard would be better positioned to understand and improve its recruitment and hiring efforts by developing metrics for recruitment of

its enlisted and all civilian cyberspace personnel. Further, using these metrics would help the Coast Guard to assess the effectiveness of its recruitment and hiring process for these personnel.

### Retention: Two of Three Selected Leading Practices Are Partially or Not Implemented

Of the three selected retention leading practices, the Coast Guard fully implemented one, partially implemented one, and did not implement one for its cyberspace workforce. Table 2 summarizes our assessment of the Coast Guard’s implementation of each of the three selected retention leading practices.

**Table 2: Assessment of the Coast Guard’s Implementation of Three Selected Retention Leading Practices for Its Cyberspace Workforce**

Selected Retention Leading Practice	Assessment	Explanation
1. Use data to determine key performance objectives and goals, which enable the agency to evaluate the successes of its retention approaches.	●	While the Coast Guard has data on its retention approaches for its officer, enlisted, and civilian cyberspace workforce, it has not evaluated the successes of its retention approaches. It also has not quantified or set specific retention goals and objectives across the cyberspace workforce.
2. Establish and track metrics of success for improving personnel morale, and report to agency leadership on the progress of improving morale.	○	Coast Guard officials told us that the service had not established or tracked metrics of success for improving cyberspace workforce morale. Since the Coast Guard did not have metrics, they are unable to report improvement of morale to Coast Guard leadership.
3. Provide financial incentives, such as retention allowances, to workers who obtain job-related degrees and certifications, provide student loan repayments, work-life programs and other existing pay authorities.	●	From fiscal years 2019 through 2021, the Coast Guard provided over \$9 million in retention incentives to both military and civilian cyberspace personnel. This includes retention incentives to: cyberspace officers that commit at least 4 years of service; enlisted personnel who have skills critical to the Coast Guard and who have obtained critical cyber certifications; and civilian personnel who obtained critical cyber certifications. <sup>a</sup>

- Fully implemented = Coast Guard information demonstrated all aspects of the applicable leading practice.
- Partially implemented = Coast Guard information demonstrated some, but not all, aspects of the applicable leading practice.
- Not implemented = Coast Guard information did not demonstrate any aspects of the applicable leading practice.

Source: GAO analysis of Coast Guard data and documentation. | GAO-22-105208.

<sup>a</sup>The Coast Guard provided various retention incentives to cyberspace personnel from fiscal years 2019 through 2021. For example, on the military side, it provided cyberspace officers about \$2.5 million in retention incentives to commit at least 4 years of service. It also provided about \$4.9 million from fiscal year 2019 through 2021 to enlisted personnel who have skills critical to the Coast Guard and who have obtained critical cyber certifications. On the civilian side, the Coast Guard provided about \$1.7 million from fiscal year 2020 through 2021 to civilian personnel who obtained critical cyber certifications.

### Evaluating Retention Successes

According to Coast Guard documentation, the Coast Guard’s stated goal is to “maximize retention” among its cyberspace workforce. However, it

---

has not quantified this goal with specific numbers or defined it with specific objectives.

The Coast Guard uses workforce planning teams to propose to leadership monetary and non-monetary interventions for cyberspace personnel. For example, in fiscal year 2021, Coast Guard data on its retention approaches show that it approved \$1.54 million in retention bonuses for 31 cyberspace officers and \$3.4 million to 39 enlisted cyberspace personnel as retention bonuses. In addition, data show the Coast Guard provided \$962,121 to 51 civilian cyberspace personnel in fiscal year 2021 for obtaining a cyber related certification.

Coast Guard officials stated that the service did not have quantified goals or objectives for retaining personnel because the specific number is fluid and changes from year to year for both enlisted and officer personnel. In addition, they stated that for civilian cyberspace personnel their goal is to maximize available resources, minimize vacancies, and fill positions to the extent possible. However, according to the leading practices we identified, having quantifiable goals and objectives would better inform Coast Guard officials on the effectiveness of its current retention approaches. Such an approach could potentially identify needed actions to enable changes to increase its retention of personnel. By setting and quantifying retention goals and objectives for its cyberspace workforce, the Coast Guard would be better able to evaluate the success of its retention approaches.

## Establishing and Tracking Morale

Coast Guard officials told us that any tracking of morale is the responsibility of the individual Coast Guard units. They said Coast Guard units use morale committees and non-appropriated funds to promote morale activities.

To monitor the workplace culture, the Coast Guard has used the Defense Organizational Climate Survey (Defense Climate Survey), a DOD program.<sup>36</sup> However, in 2021, we reported that these Defense Climate Surveys provide point-in-time data that are not designed to assess unit

---

<sup>36</sup>The Defense Climate Survey contains two questions to assess personnel morale. The two questions are: (1) Overall, how would you rate the current level of morale in your unit, and (2) Overall, how would you rate your own current level of morale.

---

morale over time.<sup>37</sup> To track progress made on improving morale, it is important to be able to track data over several years, rather than one point in time. In addition, in 2018, DOD put a moratorium on reporting the Defense Climate Survey data from across multiple units.<sup>38</sup>

Given that the Defense Climate Survey is not an appropriate method for tracking morale over time, it is important that the Coast Guard identify an alternative method for assessing morale of the cyberspace workforce. Coast Guard officials stated that they do not measure and track the morale of the entire cyberspace workforce. By establishing and tracking metrics of success for improving its cyberspace workforce morale, and reporting its progress to leadership, the Coast Guard would have information to address cyberspace morale issues. It would also allow the Coast Guard to determine progress made on improving cyberspace personnel morale.

---

### Training: All Four Selected Leading Practices Fully Implemented

The Coast Guard fully implemented all four selected training leading practices for its cyberspace workforce. Table 3 summarizes our assessment of the Coast Guard's implementation of each of these four practices.

---

<sup>37</sup>GAO, *Defense Nuclear Enterprise: DOD Can Improve Processes for Monitoring Long-Standing Issues*, [GAO-21-486](#) (Washington, D.C.: Aug. 18, 2021). According to Defense Equal Opportunity Management Institute officials, the purpose of the Defense Climate Surveys is to aid commanders in addressing challenges in real-time while performing their command role, rather than to drive policy.

<sup>38</sup>The moratorium suspends the ability to summarize the climate survey across multiple units. Department of Defense, *Defense Equal Opportunity Management Institute Organizational Climate Survey Aggregated Reports*, (Oct. 26, 2018). The Coast Guard Civil Rights Manual requires units, directorates, and offices with at least 16 members to administer a Defense Climate Survey within 180 calendar days of a change-of-command or change in directorate or office head, and at least annually thereafter. Coast Guard, *U.S. Coast Guard Civil Rights Manual*, COMDTINST M5350.4E (Oct. 21, 2020).

**Table 3: Assessment of the Coast Guard’s Implementation of Four Selected Training Leading Practices for its Cyberspace Workforce**

Selected Training Leading Practice	Assessment	Explanation
1. Establish a training and development program to assist the agency in achieving its mission and goals.	●	The Coast Guard has an arrangement with the Department of Defense (DOD) to provide training and development to Coast Guard cyberspace personnel. Officials said the Coast Guard has been able to train the workforce they need in a timely manner, and reported no challenges with using DOD training.
2. Establish working relationships with educational institutions, professional organizations, training organizations, and other experts to expand the pipeline of skilled cybersecurity talent.	●	The Coast Guard has established working relationships with various educational institutions and external agencies to expand a skilled cyberspace workforce. External training options are available to both military (enlisted and officer) and civilian cyberspace personnel. This ensures the Coast Guard provides its cyberspace personnel with a training system.
3. Collect and assess performance data (including qualitative or quantitative measures, as appropriate) to determine how the training program contributes to improved performance and results.	●	The Coast Guard collects and assesses performance data by conducting evaluations on training courses. The Coast Guard has four levels of evaluations to ensure its training program contributes to improved performance and results. Coast Guard officials said that they review challenges that are reported in the participant evaluations, including those with the classroom and with skills taught. Additionally, the Coast Guard has a process for establishing new training to improve programmatic performance. This process helps to improve performance through training, according to Coast Guard officials.
4. Use tracking and other control mechanisms to ensure that personnel receive appropriate training and meet certification requirements, when applicable.	●	The Coast Guard tracks and ensures personnel receive appropriate training and meet certification requirements through its Competency Management System, which compares competencies required by positions and competencies held by personnel. This ensures that cyberspace personnel have the required certifications and competencies for their positions.

- Fully implemented = Coast Guard information demonstrated all aspects of the applicable leading practice.
- ◐ Partially implemented = Coast Guard information demonstrated some, but not all, aspects of the applicable leading practice.
- Not implemented = Coast Guard information did not demonstrate any aspects of the applicable leading practice.

Source: GAO analysis of Coast Guard data and documentation. | GAO-22-105208.

---

## Conclusions

The Coast Guard has considered cyberspace an operational domain since 2015 and is increasingly dependent on its cyberspace workforce to implement its operations, including protecting the maritime transportation system from cyberattacks. Since the cyberspace operational domain has growing mission demands, understanding the necessary staffing levels and skills the service requires to meet its cyber related mission needs is essential—for the Coast Guard and the maritime transportation system. By assessing and determining the cyberspace staffing levels it needs, the Coast Guard can fully understand the resources it requires, including those to protect its information systems and data from threats.

Although central to effectively managing its cyberspace workforce, the Coast Guard has not developed a strategic workforce plan for this segment of the workforce, or fully used data and metrics to guide its planning efforts. Without having such a plan—that includes strategies and implementing activities to address all cyberspace competency and staffing needs—the Coast Guard will likely miss opportunities to recruit for difficult-to-fill cyberspace positions, a problem that has worsened in recent years. In addition, incorporating data from its new Cyber Mission Specialist rating into its strategic workforce planning would put the Coast Guard in a better position to plan for its enlisted cyberspace workforce. Further, developing metrics and using them to assess the effectiveness of its enlisted and all civilian cyberspace workforce recruitment and hiring process, would better position the Coast Guard to understand and improve these efforts.

Finally, setting and quantifying specific retention goals and objectives for its cyberspace workforce would help the Coast Guard better evaluate the success of its retention approaches. Additionally, efforts to improve morale in the cyberspace workforce are important to retaining these personnel. By establishing and tracking metrics of success for improving its cyberspace workforce morale, and reporting its progress to leadership, the Coast Guard would have information to address cyberspace morale issues. It would also allow the Coast Guard to determine any progress made on improving morale.

---

## Recommendations for Executive Actions

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

The Commandant of the Coast Guard should assess and determine the staffing levels needed to meet its cyberspace mission demands.  
(Recommendation 1)



---

The Commandant of the Coast Guard should establish a strategic workforce plan for its cyberspace workforce, to include strategies and implementing activities to address all competency and staffing needs. (Recommendation 2)

The Commandant of the Coast Guard should incorporate data from the Cyber Mission Specialist rating to inform its strategic workforce planning for the enlisted cyberspace workforce. (Recommendation 3)

The Commandant of the Coast Guard should develop metrics for recruitment of enlisted and all civilian cyberspace personnel, and use these metrics to assess the effectiveness of its recruitment and hiring efforts. (Recommendation 4)

The Commandant of the Coast Guard should set and quantify retention goals and objectives for its cyberspace workforce. (Recommendation 5)

The Commandant of the Coast Guard should establish and track metrics of success for improving cyberspace personnel morale and report its progress to Coast Guard leadership. (Recommendation 6)

---

## Agency Comments and Our Evaluation

We provided a draft of this report to DHS and the Coast Guard for review and comment. In its comments, reproduced in full in appendix I, DHS concurred with our six recommendations and described actions planned to address them. DHS and the Coast Guard also provided technical comments, which we incorporated as appropriate.

DHS concurred with our first five recommendations and described planned actions to address them. For example, DHS stated that the Coast Guard anticipates completing a Manpower Requirements Analysis for its Cyber Command in August 2023 and plans to identify stakeholders and resources to assess options for additional analysis of the remaining cyberspace workforce. In addition, the Coast Guard's Office of Cyberspace Forces plans to complete a workforce management plan that will address the maturation of the Coast Guard's operational cyber workforce. DHS estimated completing this action by September 29, 2023.

With regard to our sixth recommendation, DHS reiterated that the Coast Guard uses DOD's Defense Climate Survey to report unit-level climate results to unit leadership. They said the tool provides commanders with specific information on critical personnel topics so that they can take immediate steps to improve their command climate. In addition, they said Coast Guard commanders of cyber units, including the Office of

---

Cyberspace Forces, C5I Service Center, and Cyber Command, are required to use the Defense Climate Survey annually to assess the command climate. Further, DHS stated that this tool includes a survey of workforce climate and morale status. However, as we discussed earlier, in 2021 we reported that these Defense Climate Surveys provide point-in-time data that are not designed to assess unit morale over time or drive policy. Given that the Defense Climate Survey is not an appropriate method for tracking morale over time, it is important that the Coast Guard identify an alternative method for assessing morale of the cyberspace workforce.

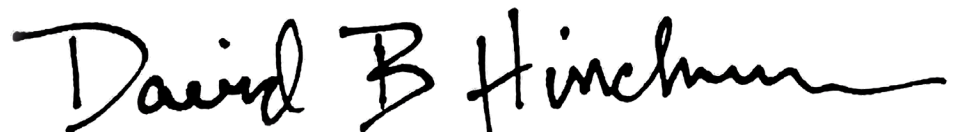
---

We are sending copies of this report to the appropriate congressional committees, the Secretary 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 staffs have any questions about this report, please contact Heather MacLeod at 202-512-8777 or [macleodh@gao.gov](mailto:macleodh@gao.gov) or David Hinchman at 214-777-5719 or [hinchmand@gao.gov](mailto:hinchmand@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 that made key contributions to this report can be found in appendix II.



Heather MacLeod  
Acting Director, Homeland Security and Justice Issues



David Hinchman  
Acting Director, Information Technology and Cybersecurity

# Appendix I: Comments from the Department of Homeland Security

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



**Homeland  
Security**

September 14, 2022

Ms. Heather MacLeod  
Acting Director, Homeland Security and Justice  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

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

Re: Management Response to Draft Report GAO-22-105208, "COAST GUARD:  
Workforce Planning Actions Needed to Address Growing Cyberspace Mission  
Demands"

Dear Ms. MacLeod and Mr. Hinchman:

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 Coast Guard has made efforts to plan and manage its cyberspace workforce, such as by fully or partially implementing 10 out of 12 recruitment, retention, and training leading practices selected by the GAO. GAO also acknowledged that the Coast Guard fully implemented four leading practices for cyberspace workforce training, including establishing a training and development program, and collecting and assessing performance data. By launching the: (1) Cyber Command in 2013; (2) Cyber Domain in 2015; and (3) Command, Control, Communications, Computers, Cyber, and Intelligence (C5I) Service Center in 2020, and considering several other initiatives underway, the Coast Guard has clearly demonstrated its commitment to progressive planning and improvements for its cyberspace workforce.

---

**Appendix I: Comments from the Department of  
Homeland Security**


---

The draft report contained six 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: 2022.09.14 08:05:48 -04'00'

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

Enclosure

**Enclosure: Management Response to Recommendations  
Contained in GAO-22-105208**

GAO recommended that The Commandant of the Coast Guard:

**Recommendation #1:** Assess and determine the staffing levels needed to meet its cyberspace mission demands.

**Response:** Concur. On August 19, 2022, The Coast Guard's Office of Cyberspace Forces (CG-791) initiated a Manpower Requirement Analysis (MRA) for CGCYBER Command, which is currently being conducted by the Office of Strategy and Human Resource Capability (CG-1B) and is anticipated to be complete in August 2023. Separately, the Cyber Workforce Integrated Planning Team (IPT) will identify stakeholders and resources to assess options for additional analysis of the remaining cyberspace workforce. Estimated Completion Date (ECD): September 29, 2023.

**Recommendation #2:** Establish a strategic workforce plan for its cyberspace workforce, to include strategies and implementing activities to address all competency and staffing needs.

**Response:** Concur. CG-791 is currently drafting a Workforce Management Plan which, once complete, will address the maturation of the Coast Guard's operational cyber workforce. This plan is a collaborative effort within the Cyber Workforce IPT. ECD: September 29, 2023.

**Recommendation #3:** Incorporate data from the Cyber Mission Specialist [CMS] rating to inform its strategic workforce planning for the enlisted cyberspace workforce.

**Response:** Concur. CG-791, in collaboration with the Office of Workforce Forecasting and Analysis (CG-126), will incorporate data gathered from the CMS rating into workforce planning efforts. Specifically, implementation of the CMS rate begins in fiscal year (FY) 2023, and once the CMS rate is fully implemented in FY 2025, CG-791 and CG-126 will use that data to inform the mission-based capabilities requirements, to determine the number and the type of positions required for the cyberspace workforce to accomplish the Coast Guard's missions in the cyberspace domain. ECD: September 30, 2026.

**Recommendation #4:** Develop metrics for recruitment of enlisted and all civilian cyberspace personnel, and use these metrics to assess the effectiveness of its recruitment and hiring efforts.

---

**Appendix I: Comments from the Department of  
Homeland Security**

---

**Response:** Concur. The Directorate of Civilian Human Resources, Diversity, and Leadership (CG-12) and the Coast Guard Recruiting Command currently measure workforce health and adjust the Coast Guard's recruiting goals based on the service's workforce needs. Once the Cyber Mission Specialist rate (beginning in FY 2023) is fully implemented in FY 2025, CG-12 and the Coast Guard Recruiting Command will track cyberspace workforce metrics. ECD: September 30, 2026.

**Recommendation #5:** Set and quantify retention goals and objectives for its cyberspace workforce.

**Response:** Concur. The Coast Guard's Workforce Planning Team currently measures workforce health, and adjusts its goals based on the service's retention as applicable to each of the workforce's specialized rates. Once the Cyber Mission Specialist rate (beginning in FY 2023) is fully implemented in FY 2025, the Assistant Commandant for Human Resources Workforce Planning Team will track cyberspace workforce metrics and consider retention incentives. ECD: September 30, 2026.

**Recommendation #6:** Establish and track metrics of success for improving cyberspace personnel morale and report its progress to Coast Guard leadership.

**Response:** Concur. The Coast Guard currently uses the Defense Organizational Climate Survey (DEOCS), which is a unit-level climate tool with results reported directly to unit leadership, and provides commanders with specific information on critical personnel topics so that they can take immediate steps to improve their command climate. As per the Coast Guard Civil Rights Manual, COMDTINST M5350.4 (series), dated October 21, 2020,<sup>1</sup> Coast Guard Commanders of Cyber units (to include, CG-791, the Command, Control, Communication, Computer, Cyber and Intelligence Service Center, CGCYBER) are required to use the DEOCS annually to assess command climate. This tool includes a survey of workforce climate and morale status.

DHS requests that GAO consider this recommendation resolved and closed, as implemented.

---

<sup>1</sup> <https://www.uscg.mil/Portals/0/Headquarters/civilrights/PDFs/USCG-Civil-Rights-Manual-COMDTINST-M5350-4E.pdf?ver=t78ky-ihps4Qfv3il3HTng%3D%3D&timestamp=1606241049129>

---

# Appendix II: GAO Contacts and Staff Acknowledgments

---

## GAO Contacts

Heather MacLeod at 202-512-8777 or [macleodh@gao.gov](mailto:macleodh@gao.gov) or  
David Hinchman at 214-777-5719 or [hinchmand@gao.gov](mailto:hinchmand@gao.gov).

---

## Staff Acknowledgements

In addition to the contacts named above, Jason Berman (Assistant Director), Tammi Kalugdan (Assistant Director), Emily Hutz (Analyst-in-Charge), Ben Crossley, Erika Cubilo, Matthew Gray, Dave Hooper, Jeff R. Jensen, Ahsan Nasar, Dwayne Staten, Gifty Owusu-Tawiah, Mary Turgeon, Walter Vance, and Adam Vogt 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.

---

## 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](mailto: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](mailto: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](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington, DC 20548

