United States Government Accountability Office

Report to Congressional Committees

September 2025

DOD CYBERSPACE OPERATIONS

About 500 Organizations Have Roles, with Some Potential Overlap

GAO-25-107121

GAO Highlights

DOD CYBERSPACE OPERATIONS

About 500 Organizations Have Roles, with Some Potential Overlap

GAO-25-107121 September 2025

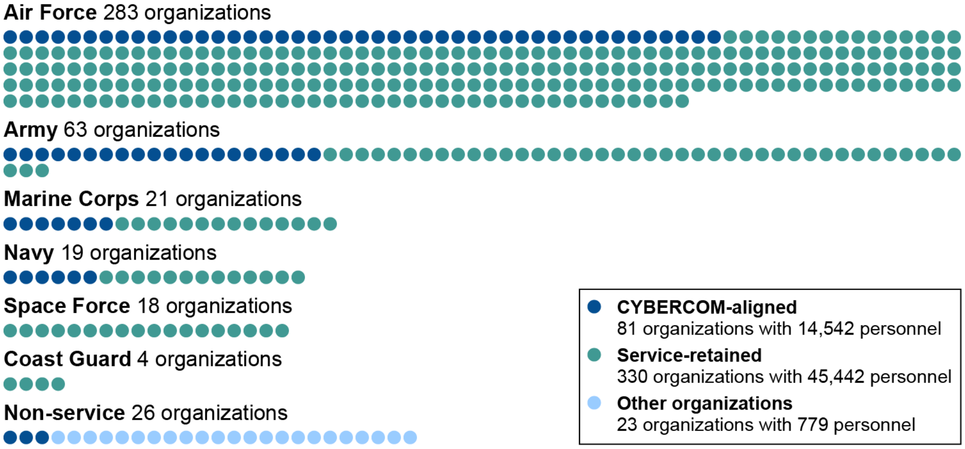
A report to congressional committees.

For more information, contact: Joseph W. Kirschbaum, kirschbaumj@gao.gov

What GAO Found

According to data provided by Department of Defense (DOD) components, DOD has established almost 440 organizations that contain about 61,000 military and civilian personnel (and over 9,500 contractors), to conduct cyberspace operations. These organizations are most often aligned with U.S. Cyber Command (CYBERCOM) or retained by the military services and conduct a mixture of offensive, defensive, and DOD Information Network operations (see figure). CYBERCOM-aligned organizations include organizations such as Navy cyber strike activities and Army cyber protection battalions that oversee tactical Cyber Mission Force teams. Military service organizations include units such as Air Force communications squadrons and Marine Corps radio battalions. Other organizations include cybersecurity service providers that provide network protection services to non-service components, such as the Defense Threat Reduction Agency and the Defense Advanced Research Projects Agency.

Department of Defense Organizations Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

To enable organizations conducting cyberspace operations, each unit is supported by organizations providing budgetary, personnel, policy, and training support. GAO identified 70 organizations and about 3,400 personnel that provide support to cyberspace operations. These include the Office of the Secretary of Defense, military department, and service headquarters, and other organizations.

GAO found that some of the functions of these organizations may overlap. These include training courses the military services provide to organizations conducting cyberspace operations and the administration of DOD's 23 cybersecurity service providers that conduct cybersecurity for DOD organizations. Although some overlap can be intentional and appropriate, unnecessary overlap can lead to organizations paying for the same service or product twice or more. As DOD considers the future organization and composition of its cyberspace operations forces, it will be important to take steps to reduce cost and inefficiencies while maintaining mission effectiveness.

Why GAO Did This Study

The U.S. and its allies face sophisticated cyber threats from both state and nonstate actors. To counter these threats, DOD conducts cyberspace operations to defend the nation, support allies and partners, and protect its DOD Information Network.

Conference Report 118-301 includes a provision for GAO to review DOD's management of cyberspace operations. GAO (1) identified the type and number of organizations and personnel that conduct cyberspace operations and (2) evaluated the extent to which there is overlap between organizations that provide budgetary, personnel, policy, or training support for cyberspace operations.

GAO reviewed relevant documents, including DOD guidance, Secretary of Defense memorandums, and organizational command briefs. GAO collected and analyzed data from 434 organizations conducting and 70 organizations supporting cyberspace operations that were identified with DOD. GAO also interviewed relevant officials, such as those from the offices of the DOD and the military services' principal cyber advisors.

What GAO Recommends

GAO is recommending that DOD assess whether (1) similar cyberspace training courses provided by the services can be consolidated and (2) there are opportunities to increase mission effectiveness and cost savings by consolidating DOD cybersecurity service providers. DOD concurred with both recommendations and identified actions it will take to implement them.

Contents

Letter 1

Background 4
About 440 DOD Organizations Conduct Cyberspace Operations 7
Some DOD Organizations Provide Similar Support to Cyberspace Operations 14
Conclusions 20
Recommendations for Executive Action 21
Agency Comments and Our Response 21

Appendix I Objectives, Scope, and Methodology 24

Appendix II U.S. Cyber Command (CYBERCOM) Cyberspace Operations 29

Appendix III Army Cyberspace Operations 33

Appendix IV Navy Cyberspace Operations 37

Appendix V Marine Corps Cyberspace Operations 41

Appendix VI Air Force Cyberspace Operations 45

Appendix VII Space Force Cyberspace Operations 49

Appendix VIII Cybersecurity Service Provider (CSSP) Cyberspace Operations 52

Appendix IX Comments from the Department of Defense 56

Appendix X GAO Contact and Staff Acknowledgments 58

Tables

Table 1: Number of Service-Retained Organizations Conducting Cyberspace Operations (Including Personnel and Contractors) 11
Table 2: Organizations in Each Military Service Providing Budgetary, Personnel, Policy, and Training Support 16
Table 3: Service Organizations Aligned with U.S. Cyber Command's (CYBERCOM) Cyberspace Operations 30
Table 4: Number of Personnel and Contractors in Cyber Mission Force Teams 32
Table 5: Department of Defense (DOD) Cybersecurity Service Providers (CSSP) 53

Figures

Figure 1: Cyberspace Operations Missions and Actions 5
Figure 2: Summary of DOD Organizations Conducting Cyberspace Operations 8
Figure 3: Summary of U.S. Cyber Command (CYBERCOM) Aligned Organizations Conducting Cyberspace Operations 9
Figure 4: Summary of Service-Retained Organizations Conducting Cyberspace Operations 11
Figure 5: Number of DOD Military and Civilian Personnel Providing Budgetary, Personnel, Policy, Training Support 14
Figure 6: Number of U.S. Cyber Command (CYBERCOM) Organizations Conducting Cyberspace Operations 29
Figure 7: U.S. Cyber Command Organizational Construct 31
Figure 8: Number of Army Organizations Conducting Cyberspace Operations 33
Figure 9: Army Organizations and Associated Personnel That Conduct Cyberspace Operations 34
Figure 10: Number of Army Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support 36
Figure 11: Navy Organizations and Personnel Conducting Cyberspace Operations 37
Figure 12: Navy Organizations and Associated Personnel That Conduct Cyberspace Operations 38

Figure 13: Number of Navy Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support 40
Figure 14: Marine Corps Organizations and Personnel Conducting Cyberspace Operations 41
Figure 15: Marine Corps Organizations and Associated Personnel That Conduct Cyberspace Operations 42
Figure 16: Number of Marine Corps Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support 44
Figure 17: Air Force Organizations and Personnel Conducting Cyberspace Operations 45
Figure 18: Air Force Organizations and Associated Personnel That Conduct Cyberspace Operations 46
Figure 19: Number of Air Force Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support 48
Figure 20: Space Force Organizations and Personnel Conducting Cyberspace Operations 49
Figure 21: Space Force Organizations and Associated Personnel That Conduct Cyberspace Operations 50
Figure 22: Number of Space Force Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support 51
Figure 23: Number of Cybersecurity Service Provide (CSSP) Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support 55

Abbreviations

CMF	Cyber Mission Force
CSSP	cybersecurity service provider
CYBERCOM	U.S. Cyber Command
DOD	Department of Defense
DODIN	Department of Defense Information Network
RFI	Request for Information

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

September 17, 2025

Congressional Committees

The United States and its allies face sophisticated cyber threats from both state and nonstate actors.[1] Russia conducted cyberspace attack activities in the days prior to and after invading Ukraine on February 24, 2022. In 2024, U.S. government agencies assessed that cyber actors (including an organization known as “Volt Typhoon”) sponsored by the People’s Republic of China are seeking to preposition themselves on information technology networks for disruptive or destructive cyber activities against U.S. critical infrastructure in the event of a major crisis or conflict with the United States.[2] In another assessment, agencies noted that Iranian cyber actors were compromising organizations across multiple U.S. critical infrastructure sectors, including the health care, public health, government, information technology, engineering, and energy sectors.[3]

These malicious cyber actors take actions to steal intellectual property from U.S. businesses and health care data; hold hostage or expose data for criminal enterprises; conduct espionage against U.S. government systems; exploit vulnerabilities in blockchain technology and steal virtual currency; and position themselves to cripple U.S. critical infrastructure at a time of their choice.[4] Given such actions, the Department of Defense (DOD) conducts cyberspace operations to defend the nation, prepare to

[1] General Timothy D. Haugh, Commander, United States Cyber Command, posture statement before the Senate Committee on Armed Services, 118th Cong., Apr. 10, 2024.

[2] Joint Cybersecurity Advisory, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, AA24-038A, Feb. 7, 2024.

[3] Joint Cybersecurity Advisory, *Iranian Cyber Actors’ Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations,* AA24-290A, Oct. 16, 2024.

[4] Adam Meyers, Senior Vice President, Counter Adversary Operations, CrowdStrike; Rear Admiral Mark Montgomery, U.S. Navy (Ret.), Senior Director, Center on Cyber and Technology Innovation, Foundation for Defense of Democracies; and Kemba Walden, President, Paladin Global Institute, *Unconstrained Actors: Assessing Global Cyber Threats to the Homeland*, testimony before the House Committee on Homeland Security, 119th Cong., 1st sess., Jan. 22, 2025.

fight and win the nation’s wars, and protect the cyber domain with allies and partners.[5]

To conduct these DOD-led cyberspace operations, components across the department have established offices, units, and commands responsible for these activities. In addition to units that are established (in part or whole) specifically for conducting cyberspace operations, there are DOD and contractor personnel who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not cyberspace operations. For example, the Navy identified more than 3,000 positions of sailors who conduct cyberspace operations (such as DOD information network operations) while aboard Navy ships; however, those positions are assigned to the ship and not an organization that conduct cyberspace operations. We did not include these individuals within the scope of this report as DOD did not have a way to identify them consistently and reliably.

DOD cyberspace operations units and commands are supported through the respective DOD component’s budget, policy, personnel, and training offices, units, and commands. DOD considers cyberspace activities—which include cyberspace operations, cybersecurity, and cyber research and development—a high priority. The department included $14.5 billion for cyberspace activities in its fiscal year 2025 budget request and has taken or is undertaking efforts to improve its cyberspace operations. For example, the department established a new policy official for cyber operations—the Assistant Secretary of Defense for Cyber Policy—who is responsible for all matters related to cyber-related activities that support or enable DOD cyberspace missions as required by section 901 of the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023.[6]

DOD is also considering several proposals to shape the future of its cyberspace forces, including how DOD generates, trains, and organizes for maximum effect. Complicating these efforts, however, is that DOD cyberspace operations are complex and operational command and control cuts across more than two dozen DOD components. As DOD and Congress consider proposals regarding the future of DOD’s cyberspace

[5] According to Chairman of the Joint Chiefs of Staff’s Joint Pub*. 3-12 Joint Cyberspace Operations* (Dec. 19, 2022), cyberspace operations are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace.

[6] Pub. L. No. 117-263, § 901 (2022).

forces, it will be important that they have credible information regarding the size, organization, and management of the department’s cyberspace operations force.

The Conference Report accompanying the National Defense Authorization Act for Fiscal Year 2024 includes a provision for us to conduct a review to identify the command staffs, secretariats, organizations, units, and personnel that conduct cyberspace operations or with any responsibility or management of budgetary, personnel, policy, or training matters affecting cyberspace operations across DOD, as well as other related issues.[7] This report (1) identifies the type and number of organizations and personnel that conduct DOD cyberspace operations; and (2) evaluates the extent to which there is overlap between organizations that provide budgetary, personnel, policy, or training support for cyberspace operations.

To address the first objective, we developed a request for information (RFI) and distributed it to 134 DOD organizations. We used this approach because DOD does not have a readily available mechanism to identify organizations, DOD personnel, or contractor personnel that conduct or support cyberspace operations. We focused on organizations that DOD officials identified as being organized for the purpose of conducting cyberspace operations and counted the personnel and contractors within those units. Through this approach, regardless of role, all personnel (military, civilian, and contractor) who were assigned to the organization would be counted. The RFI included questions regarding command-and-control relationships and whether the organization conducts offensive, defensive, or DOD Information Network (DODIN) operations. We received responses from all 134 organizations to which we sent an RFI. We also reviewed supplementary information provided by the RFI respondents, interviewed DOD officials, and conducted internet searches of DOD cyberspace organizations. In reviewing the supplementary information, we either included organizations (as is) in the scope of our review, consolidated them within another organization in our review, or removed them from the scope of our review.

Further, in reviewing this information, we identified 360 additional organizations. For these additional organizations, we did not transmit an RFI to them. Instead, we contacted them directly or organizations that had command and control over them and received data on the number of

[7] H.R. Rep. No. 118-301, at 1291-1292 (2023) (Conf. Rep.).

personnel. In all, we collected data from 494 organizations. We tabulated these data into spreadsheets and tables and presented the data to the relevant DOD officials several times. In each instance we asked the DOD officials to review the data for accuracy and completeness or provide updated data.

To address the second objective, we leveraged the RFI to also request data on the number of organizations and uniformed and DOD civilian personnel who provide budgetary, personnel, policy, or training support for cyberspace operations. While organizations that conduct cyberspace operations are supported across other areas (to include intelligence and planning support), we focused on the officials who provide budgetary, personnel, policy, and training support because those were the areas identified in the congressional provision requesting our assessment. Additionally, the RFI also asked for a list of cyberspace training courses provided by the responding organization. We consolidated and analyzed this information and reviewed any related syllabi to determine courses that were potentially providing the same training. We also interviewed agency officials to obtain their perspectives on any potential overlap in providing support to cyberspace operations and the causes and effects of such overlap.

All DOD components, except for the Army, agreed that the information in the report should be considered current as of December 31, 2024. Army officials told us that the data were current as of January 3, 2025. Additional details on our objectives, scope, and methodology can be found in appendix I.

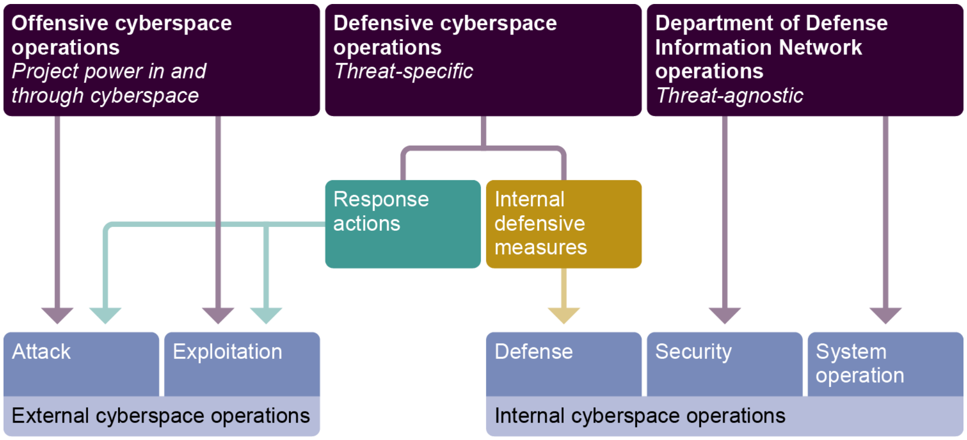
We conducted this performance audit from October 2023 to September 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions 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

Types of Cyberspace Operations

All DOD actions in cyberspace that are not simply cyberspace-enabled activities (e.g., sending an email or using the internet to take training) are taken as part of one of three cyberspace missions: (1) offensive cyberspace operations, (2) defensive cyberspace operations, or (3) DODIN operations. Like DOD missions in other domains (i.e., air, land, maritime, or space), completion of cyberspace operations missions requires the execution of specific actions. For cyberspace missions, objectives are achieved by the completion of one or more of five cyberspace actions, which are defined exclusively by the types of effects they create: attack, exploitation, defense, security, and system operation (see fig. 1).

Figure 1: Cyberspace Operations Missions and Actions


Offensive cyberspace operations
Project power in and through cyberspace
Defensive cyberspace operations
Threat-specific
Department of Defense Information Network operations
Threat-agnostic
Response actions
Internal defensive measures
Attack
Exploitation
External cyberspace operations
Defense
Security
System operation
Internal cyberspace operations

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Offensive cyberspace operations. Offensive cyberspace operations are missions intended to project power in and through cyberspace. Cyberspace attacks and cyber exploitation are the fundamental cyberspace actions of offensive cyberspace operations. These actions can include activities such as gaining unauthorized access to adversary networks, systems, and nodes of military value. Some offensive cyberspace missions may include attack actions including those that rise to the level of use of force with physical damage or destruction of enemy systems.

Defensive cyberspace operations. Defensive cyberspace operations are conducted in response to imminent or active threats and are intended to preserve the ability to use and protect cyberspace capabilities and data. Defensive cyberspace operations are used to defeat threats that have bypassed, breached, or are threatening to breach DODIN security measures. Examples of defensive cyberspace operations include internal defensive measures such as closing router ports an adversary is using for unauthorized access or blocking malware that is beaconing out of the

DODIN.[8] Additionally, defensive cyberspace operations also include response actions such as employing external countermeasures in multiple areas of responsibility to counter a large botnet (a network of computers linked together by malware).

DODIN operations. DODIN operations are operations to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and integrity of the DODIN. DODIN operations are threat agnostic in that their security measures are not focused on a specific threat. Instead, DODIN operations seek to mitigate known vulnerabilities from a broad range of threats. Further, DODIN operations seek to secure DOD cyberspace from all threats in advance of any threat activity. Examples of DODIN operations include actions taken to create and preserve the confidentiality, availability, and integrity of the DODIN, such as expeditionary forces setting up tactical networks to extend existing networks and network maintenance actions.[9]

Assistant Secretary of Defense for Cyber Policy and DOD Principal Cyber Advisor

In March 2024, DOD established the Assistant Secretary of Defense for Cyber Policy to serve as the senior official responsible for overall supervision of DOD cyberspace policy and strategy. The official establishes and oversees the implementation of DOD's cyberspace policy and strategy including those related to cyberspace forces, capabilities, and their employment. In addition, according to officials from the Assistant Secretary of Defense for Cyber Policy, the office reviews and evaluates cyber-related programs, plans, and system requirements.

The Assistant Secretary of Defense for Cyber Policy serves concurrently as the DOD Principal Cyber Advisor and oversees the DOD Principal Cyber Advisor office. The DOD Principal Cyber Advisor, in turn, is the primary advisor to the Secretary of Defense on military cyber forces and activities. The DOD Principal Cyber Advisor does not have operational responsibilities for DOD operations and is not in the operational chain of

[8] A beacon is a type of malware that systematically calls out to a specified internet protocol address or universe resource locator from a victimized system. A waiting threat agent can answer this beacon, establishing a connection that provides partial or even full remote access to the victimized system.

[9] According to Joint Pub. 3-12, "DODIN operations do not include actions taken under statutory authority of a chief information officer to provision cyberspace for operations, including information technology architecture development; establishing standards; or designing, building, or otherwise operationalizing DODIN information technology." Therefore, we did not include organizations and personnel that fall within this scope.

command. The Principal Cyber Advisor’s authority is limited to such things as the recruitment, training, assessment, and maintenance of cyberspace operations forces; and evaluating, improving, and enforcing a culture of cyberspace warfighting and accountability for cybersecurity and cyberspace operations. Further, the DOD Principal Cyber Advisor supports the Office of the Under Secretary of Defense for Acquisition and Sustainment, in the acquisition oversight, delivery, and sustainment of offensive, defensive, and DODIN cyber capabilities.

About 440 DOD Organizations Conduct Cyberspace Operations

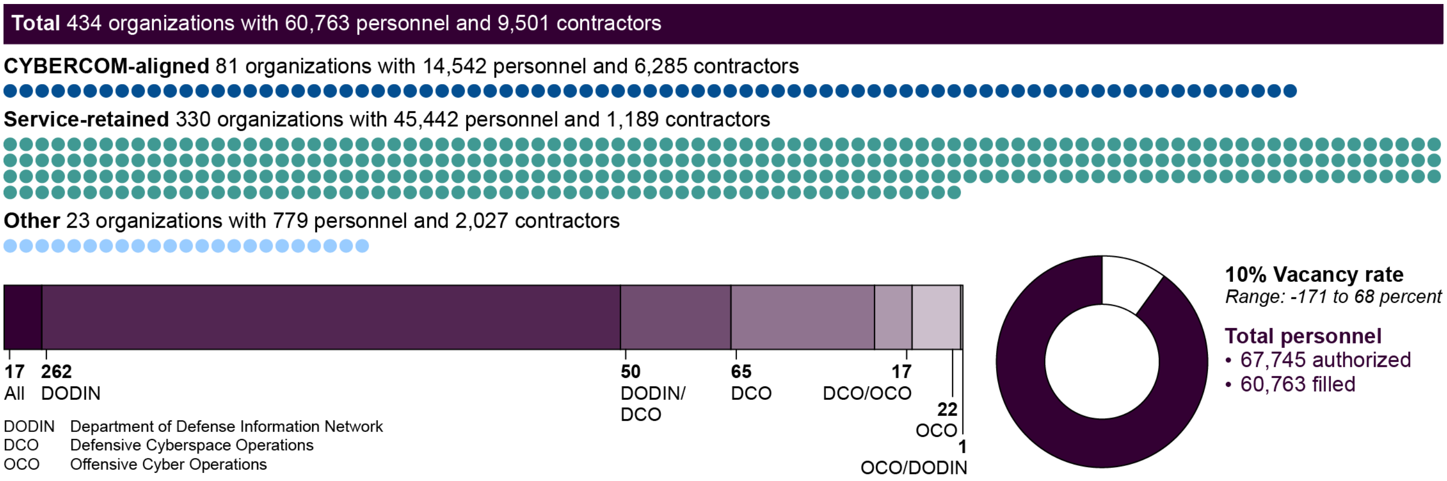
According to data provided by DOD components, DOD has established 434 organizations[10] (consisting of 60,763 personnel[11] and 9,501 contractors) that conduct cyberspace operations.[12] These organizations are either aligned within the U.S Cyber Command (CYBERCOM) command structure, retained by the military services, or not aligned with either CYBERCOM or a military service (as shown in figure 2).

[10] For purposes of this report, we used battalion- and squadron-level units as the smallest unit of measurement. The number of personnel assigned to smaller organizations—such as Cyber Mission Force (CMF) teams—is included in their respective battalion- and squadron-level units.

[11] The number of personnel currently conducting cyberspace operations represents military and civilian positions that were filled as of December 2024. We did not include authorized positions that had not been filled in our totals for personnel conducting cyberspace operations.

[12] In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractor personnel who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not cyberspace operations. For example, Marines within a Marine Corps infantry platoon or sailors on Navy ships conduct cyberspace operations (e.g., DODIN operations). Based on data components provided to us, we were able to identify at least 3,000 authorized billets that conduct cyberspace operations but are not assigned to units that conduct cyberspace operations. We did not include these individuals within the scope of this report as DOD did not have a way to identify these individuals consistently and reliably. However, DOD hopes to improve its situational awareness of these individuals as it improves its DOD cyber workforce efforts.

Figure 2: Summary of DOD Organizations Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

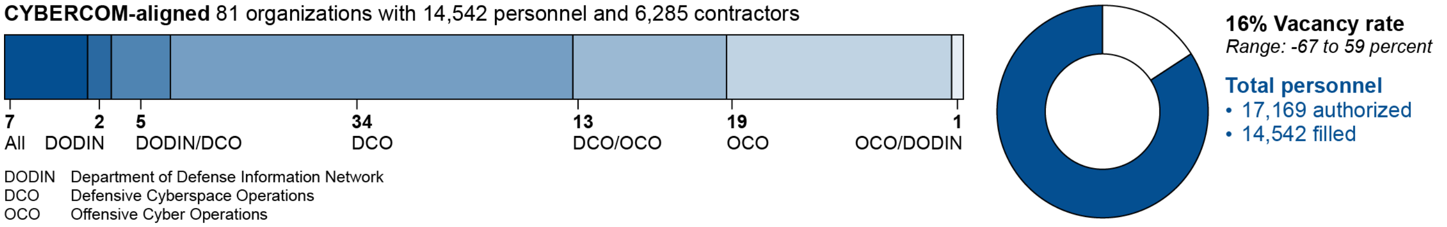
In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractors who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not to conduct cyberspace operations. For example, the Army may have personnel assigned within an Army special operations unit who conduct cyberspace operations (e.g., DODIN operations). We did not include these individuals within the scope of this report because DOD did not have a way to identify these individuals consistently and reliably.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -171 percent vacancy rate means that an organization conducting cyberspace operations reported having more than twice as many personnel than authorized (i.e., the organization reported having only 34 authorized billets but, at the same time, reported having 92 filled cyberspace operations billets). Conversely, a 68 percent vacancy rate means that an organization conducting cyberspace operations reported having filled only one-third of the personnel authorized (i.e., the organization reported having 27 authorized cyberspace operations billets, but only nine of those billets were filled).

CYBERCOM-Aligned Organizations That Conduct Cyberspace Operations

To enable CYBERCOM to direct, synchronize, and coordinate cyberspace planning and operations, DOD has established 81 organizations (consisting of 14,542 personnel and 6,285 contractors) at the strategic, operational, and tactical levels that are aligned with CYBERCOM. These organizations conduct a mixture of offensive cyberspace operations, defensive cyberspace operations, and DODIN operations (as shown in figure 3).

Figure 3: Summary of U.S. Cyber Command (CYBERCOM) Aligned Organizations Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -67 percent vacancy rate means that an organization conducting cyberspace operations reported having 67 percent more personnel than authorized (i.e., the organization reported having only 86 authorized billets but, at the same time, reported having 144 filled cyberspace operations billets). Conversely, a 59 percent vacancy rate means that an organization conducting cyberspace operations reported having filled less than half of the personnel authorized (i.e., the organization reported having 113 authorized cyberspace operations billets, but only 46 of those billets were filled).

At the strategic level, CYBERCOM defends the DODIN, supports joint force commanders with cyberspace operations, and defends the nation from significant cyberspace attacks. At the operational level, there are six headquarters organizations within CYBERCOM. These organizations include:

- Cyber National Mission Force Headquarters;
- DOD Cyber Defense Command (formerly named Joint Force Headquarters DODIN); and
- four Joint Force Headquarters-Cyber. The Joint Force Headquarters commanders also concurrently serve as the commander of their respective service cyber components.[13]

DOD Cyber Defense Command each of the four Joint Force Headquarters-Cyber commands have one or more Cyberspace Operations Integrated Planning Elements. These planning elements are staffed by the service cyber components, assigned to and co-located within different combatant commands (e.g. U.S. European Command),

[13] For example, the commander of Fleet Cyber Command is also the commander of Joint Force Headquarters-Cyber (Navy), Navy Space Command, 10th Fleet, and the Navy Service Cryptologic Component. Similarly, the commander of Air Forces Cyber is also the commander of Joint Force Headquarters-Cyber (Air Force) and 16th Air Force.

and are forward extensions of DOD Cyber Defense Command or their respective Joint Force Headquarters-Cyber.

At the tactical level, DOD established the Cyber Mission Force (CMF) to conduct CYBERCOM's key cyberspace operations missions. In April 2022, the commander of CYBERCOM stated that DOD had 133 CMF teams and planned to add 14 additional teams in the next few years. While the CMF is organized into teams for purposes of conducting operations, they are organized within service-specific organizations for administrative purposes.[14]

- Army CMF teams are organized within Cyber Battalions, Cyber Protection Battalions, Cyber Protection Centers, or Military Intelligence Battalions (Cyber). These battalions report to either a Cyber Protection Brigade or a Military Intelligence Brigade (Cyber).
- Marine Corps CMF teams report directly to either a Cyberspace Operations Battalion or the Marine Corps Cyberspace Warfare Group.
- Navy CMF teams are organized within organizations known as a Cyber Strike Activity, a Cyber Defense Activity, or Naval Information Operations Commands.
- Air Force CMF teams are organized within Cyberspace Operations Squadrons. These squadrons fall under Cyberspace Operations Groups and Cyberspace Wings.
- Space Force does not contribute personnel to CMF teams (as of January 2025).

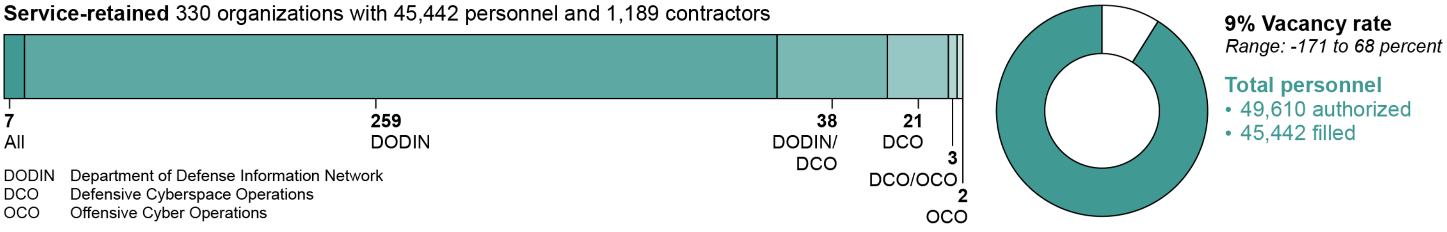
For additional details about CYBERCOM-aligned organizations, see appendix II.

Military Service-Retained Organizations That Conduct Cyberspace Operations

The military services retain hundreds of organizations to conduct offensive cyberspace operations, defensive cyberspace operations, and DODIN operations. According to data the DOD components provided, the services retain 330 organizations (consisting of 45,442 personnel and 1,189 contractors) that conduct cyberspace operations. These organizations conduct a mixture of offensive cyberspace operations, defensive cyberspace operations, and DODIN operations (as shown in figure 4).

[14] In this report, we did not count CMF teams as organizations since they are smaller than battalion- or squadron-level units. Instead, we counted the number of personnel within the CMF teams within their respective service's organization structure.

Figure 4: Summary of Service-Retained Organizations Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractors who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not to conduct cyberspace operations. For example, the Army may have personnel assigned within an Army special operations unit who conduct cyberspace operations (e.g., DODIN operations). We did not include these individuals within the scope of this report because DOD did not have a way to identify these individuals consistently and reliably.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -171 percent vacancy rate means that an organization conducting cyberspace operations reported having more than twice as many personnel than authorized (i.e., the organization reported having only 34 authorized billets but, at the same time, reported having 92 filled cyberspace operations billets). Conversely, a 67 percent vacancy rate means that an organization conducting cyberspace operations reported having filled only one-third of the personnel authorized (i.e., the organization reported having 27 authorized cyberspace operations billets but only nine of those billets were filled).

Table 1 depicts the number of military service-retained organizations conducting cyberspace operations and the associated service personnel and contractor personnel within those organizations.

Table 1: Number of Service-Retained Organizations Conducting Cyberspace Operations (Including Personnel and Contractors)

	Number of organizations[a]	Number of personnel	Number of contractors
Army	43	10,841	466
Marines	14	6,561	17
Navy	13	4,325	237
Air Force	238	22,363[b]	337
Space Force	18	1,113	62
Coast Guard	4	239	70

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Note: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

[a] Organizations include service commands, units conducting cyberspace operations, and the cybersecurity service providers within the services. For purposes of this report, we used battalion and squadron level units as the lowest level of unit we measured. Tactical level units, such as Cyber Mission Force teams, have their data reflected within battalion and squadron level organizations.

[b] Of the 22,363 Air Force-retained personnel in units conducting cyberspace operations, 20,046 individuals (90 percent) are assigned to a group of units that Air Force officials identified as being “communications squadrons” conducting DOD Information Network (DODIN) operations. Other services also have a significant number of personnel conducting DODIN operations but were not included in these totals as they are not assigned to units that were established to conduct cyberspace operations. For example, according to Navy data, there are 3,038 authorized billets tasked with conducting DODIN operations aboard Navy ships that are not assigned to units that are tasked with conducting cyberspace operations.

Examples of military service-retained units include:

- Army cyber warfare, multidomain, information operations, and signal battalions;
- Navy computer and telecommunications stations;
- Marine Corps radio and communications battalions;
- Air Force communications, engineering, cyberspace operations, and network operations squadrons; and
- Space Force cyberspace operations squadrons.

The military services also retain nine of the 23 DOD cybersecurity service providers (CSSP) that conduct cybersecurity operations. CSSPs are organizations that direct and manage network operations and provide one or more cybersecurity activities to the DODIN. The service-retained CSSPs fall into two types:

- CSSPs that conduct operations within their own services.
- CSSPs that provide services externally for other DOD components.

CSSPs generally operate under the authority and leadership of their respective commands and report information to the DOD Cyber Defense Command.

See appendixes III-VII for additional details about military service-retained cyberspace operations organizations.

Other DOD Organizations That Conduct Cyberspace Operations

In addition to establishing organizations that are aligned to CYBERCOM or that the services have retained, DOD has also established other organizations (and assigned people and hired contractor personnel) to conduct cyberspace operations. Generally, these organizations fall into one of three categories:

- **CSSPs not located within one of the military services.** According to data the DOD components provided, 14 of the 23 CSSPs (consisting of 562 personnel and 1,919 contractors) conduct cyberspace operations outside of the military services. These CSSPs include those that belong to the Defense Information Systems Agency, Defense Logistics Agency, and Missile Defense Agency.[15] See appendix VIII for additional details about CSSPs.

- **Combatant commands.** Combatant commands are responsible for securing, operating, and defending their designated DODIN area of operation (i.e., networks and systems that they authorize). The combatant commands also integrate cyberspace operations into plans. The combatant commands have organized their cyberspace operations personnel into Joint Cyberspace Centers for unity of effort in planning, coordinating, integrating, and synchronizing efforts or have designated specific individuals in different directorates throughout the command with these responsibilities. Based on data provided to us, nine of the 11 combatant commands have 209 personnel and 78 contractors that conduct cyberspace operations.[16]

- **Special operations commands and units.** U.S. Special Operations Command has a directorate within the command headquarters, at least two separate organizations that conduct cyberspace operations (including a CSSP), and personnel embedded in other organizations across the globe. Additional information about these organizations and personnel (including numbers) are classified and not included in this report.

[15] The number of personnel and contractors associated with two of the 14 CSSPs are classified and are not included in the totals reflected in this report.

[16] In addition to having Joint Cyber Centers or personnel to support combatant commander responsibilities, combatant commands also have Cyberspace Operations Integrated Planning Elements that are organizationally aligned to DOD Cyber Defense Command or one of four Joint Force Headquarters-Cyber. Since they are CYBERCOM personnel, we included them in our totals for CYBERCOM-aligned organizations.

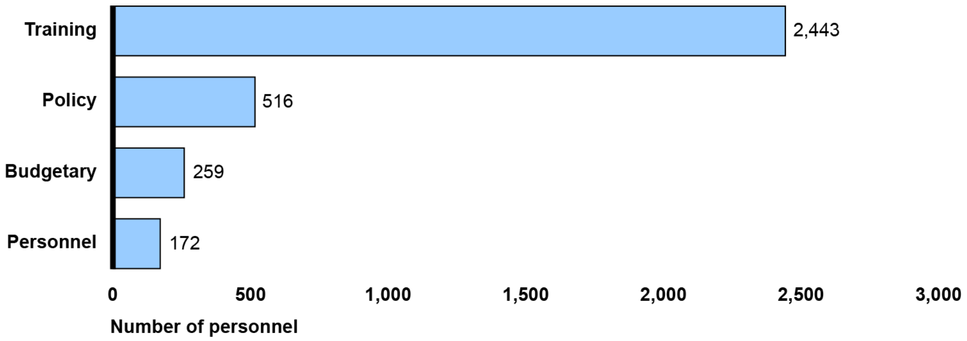
Some DOD Organizations Provide Similar Support to Cyberspace Operations

Seventy Organizations Support Cyberspace Operations

Each of the organizations conducting cyberspace operations is supported by its respective parent organization that provides budgetary, personnel, policy, and training support to cyberspace operations.

According to data DOD components provided, 70 organizations composed of 3,390 personnel provide budgetary, personnel, policy, and training.[17] Figure 5 shows the breakdown of DOD personnel supporting cyberspace operations in these four categories.

Figure 5: Number of DOD Military and Civilian Personnel Providing Budgetary, Personnel, Policy, Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Note: Support personnel can work in more than one support area. To avoid overcounting, we asked organizations to report their primary work area.

Generally, we found that this support was provided by organizations within the

- **Office of the Secretary of Defense and key offices.** These include the offices of the Assistant Secretary of Defense for Cyber Policy, the

[17] Some organizations reported both conducting and supporting cyberspace operations.

Assistant Secretary of Defense for Personnel and Readiness, the DOD Chief Information Officer, and the Office of the DOD Principal Cyber Advisor.

- **Joint Staff and combatant commands.** These include organizations from U.S. Africa Command, U.S. Northern Command, and U.S. Space Command.
- **Military department and service headquarter organizations and personnel for the military departments (Army, Navy, and Air Force).** For example, at the military department-level, the offices of the Principal Cyber Advisors and offices of the Navy and Air Force Chief Information Officer provide policy support. At the service-level, examples include the Office of the United States Marine Corps Deputy Commandant for Information and the Office of the Space Force Chief Operating Officer.
- **Military service headquarters and commands.** In several instances, an organization that conducts cyberspace operations reports to or receives support from a higher-headquarters command that is not organized to conduct cyberspace operations. For example, the Air Combat Command Headquarters staff provides support to the 16th Air Force. Also, as discussed further below, four of the five military services have training commands (and subordinate training units) that train organizations to conduct cyberspace operations.
- **DOD components with CSSPs:** Multiple DOD components and agencies provide a mix of budget, personnel, policy, and training support to their respective CSSPs. For example, the Defense Finance and Accounting Service, Defense Intelligence Agency, and Defense Threat Reduction Agency provide support to their CSSP.

While some organizations, such as the service training commands, provide a single type of support (e.g., training), the services identified other organizations that provide support in multiple capacities. For example, the Marine Corps' office of the Deputy Commandant for Information provides budgetary, personnel, and policy support to Marine Corps organizations that conduct cyberspace operations.

Areas of Overlap May Exist Between Organizations Supporting and Conducting Cyberspace Operations

Based on information that DOD components provided us, we found three areas where there may be potential overlap in the activities of organizations supporting and conducting cyberspace operations. Our prior work has found that overlap occurs when multiple agencies or programs have similar goals, engage in similar activities or strategies to achieve them, or target similar beneficiaries.[18]

Potential overlap in military services' support. First, we identified multiple organizations within each military service that are providing similar budgetary, personnel, policy, and training support to their respective organizations conducting cyberspace operations, as shown in table 2.

Table 2: Organizations in Each Military Service Providing Budgetary, Personnel, Policy, and Training Support

Military service	Organizations	Budgetary	Personnel	Policy	Training
Army	Cyber Center of Excellence Headquarters	●	●	●	●
	Cyber School				●
	Human Resources Command	●	●		
	Intelligence and Security Command Headquarters	●	●	●	
	Office of the Deputy Chief of Staff, G-3/5/7	●	●	●	●
	Office of the Deputy Chief of Staff, G-6	●	●	●	●
	Office of the Principal Cyber Advisor	●		●	
	Chief Information Officer	●		●	
	Signal School	●			●
	Cyber, Intelligence, Surveillance and Reconnaissance Center	●	●		
	Cryptologic Office	●			
Marine Corps	Office of the Deputy Commandant for Information	●	●	●	
	Training and Education Command				●
	U.S. Marine Corps Forces, Pacific	●	●	●	●
	I Marine Expeditionary Force Headquarters	●	●	●	●
	II Marine Expeditionary Force Headquarters	●	●	●	●
	III Marine Expeditionary Force Headquarters	●	●	●	●
	Marine Forces Reserve Headquarters Group		●		●
Navy	Fleet Forces Command Headquarters			●	
	Naval Information Forces Headquarters			●	●
	Office of the Chief Information Officer	●		●	
	Office of the Deputy Chief of Naval Operations for Information Warfare	●	●	●	●
	Office of the Principal Cyber Advisor	●		●	
	Center for Information Warfare Training				●
	Naval Information Warfighting Development Center	●	●		●

[18] GAO, *Fragmentation, Overlap, and Duplication: An Evaluation and Management Guide*, GAO-15-49SP (Washington, D.C.: Apr. 14, 2015).

Military service	Organizations	Budgetary	Personnel	Policy	Training
	Naval Information Warfare Training Group				●
	Naval Information Warfare Training Group Norfolk				●
	Naval Information Warfare Training Group San Diego				●
Air Force	Air Education and Training Command	●			
	Deputy Chief of Staff for Intelligence, Surveillance, Reconnaissance, and Cyber Effects Operations, A2/6	●	●	●	●
	Office of the Principal Cyber Advisor			●	
	Air Force Chief Information Officer	●		●	
	Air Combat Command Staff	●	●	●	●
	17th Training Wing				●
	333rd Training Squadron				●
	336th Training Squadron				●
	338th Training Squadron				●
	Defense Cyber Crime Center				●
	Air Force Cryptologic Office	●	●		●
	39th Information Operations Squadron				●
	318th Range Squadron				●
	275th Operations Support Squadron				●
	Reserve Headquarters	●		●	
	32nd Weapons Squadron				●
	805th Combat Test Squadron				●
Space Force	Chief Technology and Innovation Officer	●		●	
	Chief Operating Officer		●	●	
	Space Operations Command			●	
	Space Training and Readiness Command				●

Source: GAO analysis of Department of Defense data. | GAO-25-107121

Notes: The Air Force Air Education and Training Command Headquarters did not report any personnel providing training support for cyberspace operations; however, several of its subordinate units (33rd Training Squadron, 336th Training Squadron, and 338th Training Squadron) did.

Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

According to officials from the offices of Army, Navy, and Air Force principal cyber advisors, having organizations with similar support responsibilities across the military services was intentional and instituted to meet each service’s unique requirements.[19] For example, title 10 of the United States Code requires that each military service organize, train, and equip the forces assigned to it. As a result, according to the service officials, the services necessarily have their own offices and personnel to perform many key budgetary, personnel, policy, and training functions, as required. Additionally, we have recently reported, in some cases it may be appropriate or beneficial for multiple agencies or entities to be involved in the same programmatic or policy area due to the complex nature or magnitude of the federal effort.[20]

Furthermore, according to the information that was provided to us, for some organizations a significant portion of personnel providing support for cyberspace operations also provide support for activities separate from cyberspace operations. For example, officials from Space Force’s Space Operations Command reported that 100 percent of the personnel who provide policy support for cyberspace operations also support other organizational activities. Similarly, officials from the Air Force’s Cryptologic Office reported that 100 percent of the personnel who provide budget, policy, and training support for cyberspace operations also support other organizational activities. Further, officials from the Joint Staff reported that 64 percent of the personnel who provide budget, personnel, policy, and training support for cyberspace operations also support other organizational activities.

Potential overlap in military service training courses. Second, there is potential overlap in the training courses the military service training commands provide to organizations conducting cyberspace operations. For example, we identified that each military service provided a cyber defense analyst course.

According to the Office of the DOD Principal Cyber Advisor, cyberspace operations training in DOD is decentralized, and each military service is responsible for ensuring its forces meet the training requirements and standards that CYBERCOM sets. In addition, any training the military services offer must also be aligned with that respective service’s strategic objectives. As a result, according to officials, there is an incentive for the

[19] Since each military department has a principal cyber advisor, the Marine Corps and Space Force leverage the Navy’s advisor and Air Force’s advisor, according to the Navy and Air Force’s principal cyber advisor offices.

[20] GAO, *Older Americans: HHS Should Apply Leading Practices as It Coordinates Overlapping Programs*, GAO 25-107020 (Washington, D.C.: Jan. 8, 2025).

military services to develop their own cyberspace operations training programs, which creates the potential for the services to provide the same or similar foundational courses. Similarly, in responding to the draft report, the Air Force stated that potential overlap in training courses may exist since CYBERCOM joint training standards do not fully meet military service requirements for service-retained cyberspace forces.

In 2015, the Senate Armed Services Committee urged DOD to create a federated and joint training model and discouraged each service from building separate training capabilities for its respective cyber contingent.[21] As we reported in 2019, to comply with congressional direction, DOD initially moved to a joint training model, which had the principal goal to produce efficiencies and reduce training development and delivery costs. Under this model, the Army was designated as the "joint curriculum lead" for both the cyber defense analyst course and cyber operations planner course.[22] However, since that time, the services have developed potentially duplicative courses, in part, because no one within the Office of the Secretary of Defense was assessing whether the services were creating a federated and joint training model.

In 2024, DOD established the Assistant Secretary of Defense for Cyber Policy.[23] The office of the DOD Principal Cyber Advisor (within the Assistant Secretary of Defense for Cyber Policy) stated that it recognized the importance of eliminating overlap in training, but that because of the reorganization of the office, they were still developing the office's priorities. The officials added that the potential consolidation of cyberspace operations training will likely be one of the Assistant Secretary of Defense for Cyber Policy office's priorities once the reorganization is finished. Overlap in training programs could lead to DOD paying for the same thing twice or more. Additionally, the existence of multiple, similar cyberspace operations courses among the services may

[21] S. Rep. No. 114-49, at 287 (2015).

[22] GAO, *DOD Training: U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force*, GAO-19-362 (Washington, D.C.: Mar. 6, 2019).

[23] As noted in the Background section of this report, DOD established the Assistant Secretary of Defense for Cyber Policy to serve as the senior official responsible for overall supervision of DOD cyberspace policy and strategy. The official has operational responsibilities for overseeing DOD's cyberspace policy and strategy; DOD's cyberspace operations budget; and the integration of cyberspace operations and capabilities into operations and contingency plans. The Assistant Secretary of Defense for Cyber Policy serves concurrently as the DOD Principal Cyber Advisor.

indicate that DOD is not fully meeting the intent of the Senate Armed Services Committee to be efficient and reduce costs.

Potential overlap among CSSPs. Third, since there are 23 DOD CSSPs (nine aligned with the military services and 14 existing in other DOD components) conducting cyberspace operations across the department (most of which conduct DODIN operations), there may be potential areas of overlap between them and opportunities for cost savings by consolidating some functions and activities. For example, according to data DOD provided us, there are over 2,500 contractors potentially providing the same service to CSSPs and 128 personnel providing the same budget, personnel, policy, and training support to the CSSPs. Because these personnel are largely conducting the same activities and functions (i.e., providing cybersecurity services and activities to DOD organizations), there may be some opportunities for consolidation.

It is DOD policy for DOD components to continuously review manpower utilization plans and programs to ensure efficient and effective use of personnel.[24] However, the Assistant Secretary of Defense for Cyber Policy has not assessed whether consolidation of CSSPs is feasible. The Office of the DOD Principal Cyber Advisor (within the Office of the Assistant Secretary of Defense for Cyber Policy) stated that because of the recent reorganization of the office, it was still developing the office's priorities. The DOD Principal Cyber Advisor office agreed that there may be opportunities for consolidation of DOD's CSSPs, and that the Assistant Secretary of Defense for Cyber Policy office may look at the issue once the reorganization is completed. Until DOD does so, however, it may be missing opportunities to achieve cost savings and efficiencies.

Conclusions

Given sophisticated cyber threats from both state and nonstate actors, DOD has established a substantial number of organizations to conduct cyberspace operations—to include those aligned with CYBERCOM, retained by the services, or aligned with other DOD components (e.g., combatant commands). These organizations are enabled by their respective parent organization for budgetary, personnel, policy and training support; however, we found areas where there may be overlap in the activities of organizations supporting and conducting cyberspace operations. By identifying and addressing potential areas of overlap, the

[24] DOD Directive 1100.4, *Guidance for Manpower Management*, (Feb. 12, 2005).

department may achieve cost savings and reduce inefficiencies in how it supports and conducts cyberspace operations.

Recommendations for Executive Action

We are making the following two recommendations to DOD:

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Cyber Policy assesses the extent to which similar cyberspace training courses provided by the services overlap and can be consolidated to ensure that the military services are implementing a federated and joint training model in a manner that achieves efficiencies and reduces training development and delivery costs. (Recommendation 1)

The Secretary of Defense should ensure that the Assistant Secretary of Defense for Cyber Policy assesses the extent to which there are opportunities to achieve cost savings and efficiencies by consolidating DOD cybersecurity service providers. (Recommendation 2)

Agency Comments and Our Response

We provided a draft of this report for review and comment to the Department of Defense. The Department of Defense concurred with both of our recommendations and provided actions they will take to implement them. We believe these actions, if implemented, will meet the intent of our recommendations. The Department of Defense's written comments are reproduced in full in appendix IX. The Department of Defense, military departments, and U.S. Cyber Command also provided technical comments, which we incorporated as appropriate.

We are providing copies of this report to the appropriate congressional committees, the Secretary of Defense, and each of the major military components identified in this review to include the military services, Cyber Command, and select defense agencies. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact me at kirschbaumj@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 the report are listed in appendix X.

//SIGNED//

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

List of Committees

The Honorable Roger F. Wicker
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mitch McConnell
Chair
The Honorable Christopher Coons
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Ken Calvert
Chairman
The Honorable Betty McCollum
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The Conference Report accompanying the National Defense Authorization Act for Fiscal Year 2024 included a provision for us to review the Department of Defense's (DOD) management of cyberspace operations.[1] This report (1) identifies the type and number of organizations and personnel that conduct DOD cyberspace operations; and (2) evaluates the extent to which there is overlap between organizations that provide budgetary, personnel, policy, or training support for cyberspace operations.

To address objective one, we initially asked officials from the Office of the DOD Principal Cyber Advisor, the service component Principal Cyber Advisors, U.S. Cyber Command, DOD Cyber Defense Command, and the service cyber components whether they had a comprehensive list of organizations, personnel, or both that conduct or support cyberspace operations. DOD officials told us that they do not have a system that collects or maintains such information.

Since they did not have such information, we discussed different approaches to identify organizations and personnel that conduct cyberspace operations. After discussing the merits and challenges of those different options, we decided to focus on organizations that were organized to conduct cyberspace operations. Through this approach, regardless of role, all personnel (military, civilian, and contractor) who were assigned to the organization would be counted.

Leveraging information from Joint Publication 3-12, Joint Cyberspace Operations;[2] the 2019 Secretary of Defense Memorandum "Definition of Department of Defense Cyberspace Operations Forces (DoD COF);"[3] and discussions with DOD officials, we initially identified 134 cyberspace operations organizations that we planned to include in our review.

We then worked with the DOD officials to develop a request for information (RFI) that we would use to collect information about these 134 organizations. In developing the RFI questions, we consulted with the DOD officials to determine the terminology and characterization that

[1] H.R. Rep. No. 118-301, at 1291-1293 (2024) (Conf. Rep.).

[2] Joint Chiefs of Staff, Joint Pub. 3-12, Joint Cyberspace Operations (Dec. 19, 2022).

[3] In July 2025, the Secretary of Defense issued an updated memorandum which revised and superseded the 2019 definition of DOD Cyberspace Operations Forces. See Secretary of Defense Memorandum, Department of Defense Cyberspace Operations Forces (July 24, 2025).

would be most understandable to individuals completing the RFI while also meeting the intent of our assessment. A GAO survey specialist also assisted in developing the RFI questions. The RFI included questions regarding the number of personnel and organizations that conduct or support cyberspace operations. Additionally, the RFI included questions regarding command-and-control relationships and whether an organization conducts offensive, defensive, or DOD Information Network (DODIN) operations among other questions.

Regarding personnel conducting and supporting cyberspace operations, the RFI requested billet-level data. According to DOD officials, although DOD is in the process of coding its cyberspace workforce as part of the DOD Cyber Workforce Framework, this process remains incomplete, and the cyber work role codes are not uniformly implemented across the department. As a result, we requested other characteristics for each billet reported in the request for information, such as: work roles, ranks, and the number of authorized and filled billets. We transmitted the RFI to points of contact for the 134 organizations.

After the distribution of the RFI, we followed up directly with the respondents identified in the RFI to clarify the RFI questions and data requests, as needed, and answer respondent questions. For example, we coordinated with respondents to avoid double counting personnel between organizations conducting cyberspace operations and organizations supporting cyberspace operations. Additionally, in the RFI we asked organizations supporting cyberspace operations to only include personnel in one of the four areas (budgetary, personnel, policy, and training) to avoid double counting personnel whose roles may fit into more than one category. As such, we also followed up with respondents to clarify potential instances where it appeared to us that personnel were counted more than once.

Additionally, to consistently describe organizations conducting and supporting cyberspace operations, we followed up with respondents to ensure they provided information on organizations at the battalion and squadron level and above. We used battalion and squadron level units as the lowest level of unit we measured. Tactical level units, such as Cyber Mission Force teams, were directed to provide data within battalion and squadron level organizations. In instances where RFI respondents included organizations below the battalion and squadron levels in their responses, we coordinated with them to identify the relevant battalion and squadron level organizations in their chain of their command. For example, since the Cyber Mission Force teams are smaller than battalions and squadrons, we included the Cyber Mission Force personnel in the battalions, squadrons, or similar level organizations in which they are organizationally aligned. As part of the RFI, respondents were asked to provide supplementary information such as command briefs.

Ultimately through this follow-up, we received information from each organization that we initially identified. In reviewing the information, we obtained about these organizations, we either included them (as is) in the scope of our review, consolidated them within another organization in our review, or removed them from the scope of our review. In addition, after reviewing the supplementary information we requested, conducting internet searches of DOD cyberspace operations organizations, and conferring with DOD officials, we identified 360 additional organizations that conducted or supported cyberspace operations.

For these additional organizations, we did not transmit an RFI to them. Instead, we contacted them directly or organizations that had command and control over them and received data on the number of personnel. In all, we collected data from 494 organizations. In responding to our RFI, a few DOD components identified personnel who conduct cyberspace operations that were assigned to organizations that were not tasked to conduct such operations (such as a special operator who conducts cyberspace operations as a member of special operations team or a Marine who is a member of a platoon that, as a unit, is not designed to conduct cyberspace operations). Since DOD did not have way to consistently and reliably identify such personnel, we agreed to acknowledge such individuals exist but not include them in this report given data reliability issues.

To address the second objective, we leveraged the RFI to also request data on the number of organizations and uniformed and DOD civilian personnel who provide budgetary, personnel, policy, or training support for support cyberspace operations. While organizations that conduct cyberspace operations are supported across other areas (to include intelligence and planning support), we focused on the officials who provide budgetary, personnel, policy, and training support because those were the areas identified in the congressional provision requesting our assessment.

The RFI requested that respondents identify information on personnel providing support to cyberspace operations, such as the work roles, ranks, extent to which individuals supported non-cyberspace operations, and the number of authorized and filled billets. To avoid double counting individuals who may provide support to more than one of the support categories (budgetary, personnel, policy, and training), we asked respondents to place individuals in the single category most applicable to their role. The RFI did not include a request for contractor personnel providing budgetary, personnel, policy, or training support to cyberspace operations. We analyzed these data to determine the organizations within each military service that are providing similar budgetary, personnel, policy, and training support to their respective organizations conducting cyberspace operations.

Additionally, the RFI also asked for a list of cyberspace training courses provided by the responding organization. We consolidated and analyzed this information and reviewed any related syllabi to determine courses that were potentially providing the same training. For both potential areas of overlap, we interviewed officials from the DOD Principal Cyber Advisor's office and military services' principal cyber advisor offices to obtain their perspectives.

We took several steps to assess the reliability of data provided by DOD officials. For example, the RFI included questions that asked the respondents to describe the internal processes their organization used to pull the data for cyberspace operations and support personnel. We reviewed the responses to these questions and followed up via email and phone calls with respondents to obtain any clarification that was needed. While some DOD components did not respond to those questions within the RFI, we have assessed the associated risk and concluded that any potential errors resulting from the lack of data reliability response from single organizations are not substantial enough to cause a reasonable person, aware of the errors, to doubt a finding, conclusion, or recommendation supported by the data especially since we aggregated the data by DOD, military services, and components.

After collecting all the information from the 494 organizations, we manually inputted the data into Excel spreadsheets. Large data files were automatically processed into the spreadsheets by a GAO data analyst using Statistical Analysis Software. Once the data were consolidated into tables, we analyzed the data to identify odd/incorrect/missing responses. We then asked the relevant DOD officials about the questionable data and provided them an opportunity to provide comments, identity anomalies, or provide updated data. During these meetings we also asked officials to verify the accuracy and completeness of their organization's data. Updated data provided by DOD were then manually inputted into the spreadsheets. Any manually inputted data were verified back to the source document by another GAO analyst. We then conducted two exit conferences where we presented the consolidated data to the Office of the Secretary of Defense, U.S. Cyber Command, military service cyber components, Joint Staff, cybersecurity service security providers, and combatant command officials and again asked them to review the data for accuracy and completeness or provide any updates.

All DOD components, except for the Army, agreed that the information in the report should be considered current as of December 31, 2024. Army officials told us that the data were current as of January 3, 2025. In June 2025 we transmitted the draft report to DOD. Based on comments received, we modified number of organizations and personnel (to include adding a new organization and removing some personnel from the count).

Given the steps taken above to ensure the accuracy and completeness of the data, we believe that the data are sufficiently reliable for the purpose of establishing an initial estimate and baseline for the number of personnel and organizations conducting and supporting DOD's cyberspace operations.

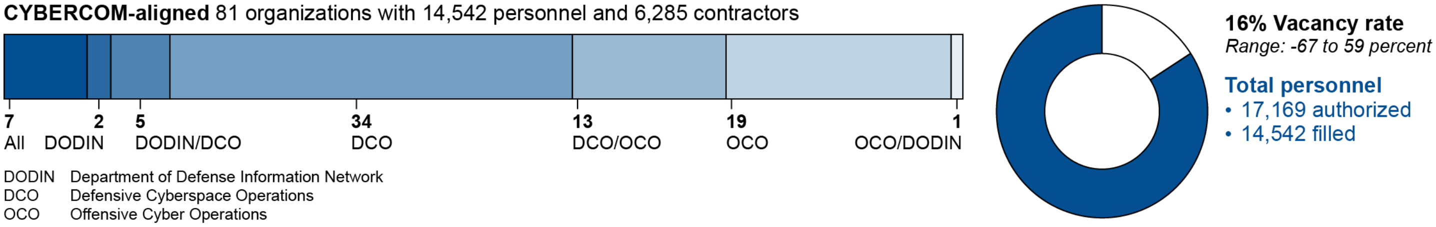
We conducted this performance audit from October 2023 to September 2025 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: U.S. Cyber Command (CYBERCOM) Cyberspace Operations

Source: U.S. Cyber Command. | GAO-25-107121

CYBERCOM and its aligned organizations—which consist of 81 organizations, 14,542 personnel, and 6,285 contractors—conduct Department of Defense (DOD) Information Network (DODIN) operations, defensive operations, and offensive operations (or some combination thereof), as shown in figure 6 below.

Figure 6: Number of U.S. Cyber Command (CYBERCOM) Organizations Conducting Cyberspace Operations



DODIN	Department of Defense Information Network
DCO	Defensive Cyberspace Operations
OCO	Offensive Cyber Operations

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -67 percent vacancy rate means that an organization conducting cyberspace operations reported having more personnel than authorized (i.e., the organization reported having only 86 authorized billets but, at the same time, reported having 144 filled cyberspace operations billets). Conversely, a 59 percent vacancy rate means that an organization conducting cyberspace operations reported having filled less than half the personnel authorized (i.e., the organization reported having 113 authorized cyberspace operations billets, but only 46 of those billets were filled).

The 81 organizations include CYBERCOM headquarters, six subordinate organizations, and service organizations that are aligned to the command.

- **CYBERCOM Headquarters** directs, synchronizes, and coordinates cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.
- **Cyber National Mission Force Headquarters** focuses on defending the nation and oversees units that conduct offensive and defensive cyberspace operations.
- **DOD Cyber Defense Command** primarily focuses on DOD-wide efforts to secure, operate, and defend the DODIN (i.e., information network operations and defensive cyberspace operations).
- **Four Joint Force Headquarters-Cyber** primarily focus on supporting the Joint Force and provide the combatant commands with direct support, cyberspace operations expertise, and reachback capability to CYBERCOM through Cyberspace Operations Integrated Planning Elements aligned to each combatant command.

The military services have 78 organizations aligned to CYBERCOM, as shown in table 3 below.

Table 3: Service Organizations Aligned with U.S. Cyber Command's (CYBERCOM) Cyberspace Operations

	Number of organizations	Number of personnel[a]	Number of contractors	Additional information
Army	20	5,056	3,129	Appendix III
Navy	6	2,416	105	Appendix IV
Marine Corps	7	2,017	1,521	Appendix V
Air Force	45	3,751	27	Appendix VI
Space Force[a]	0	0	0	Appendix VII

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

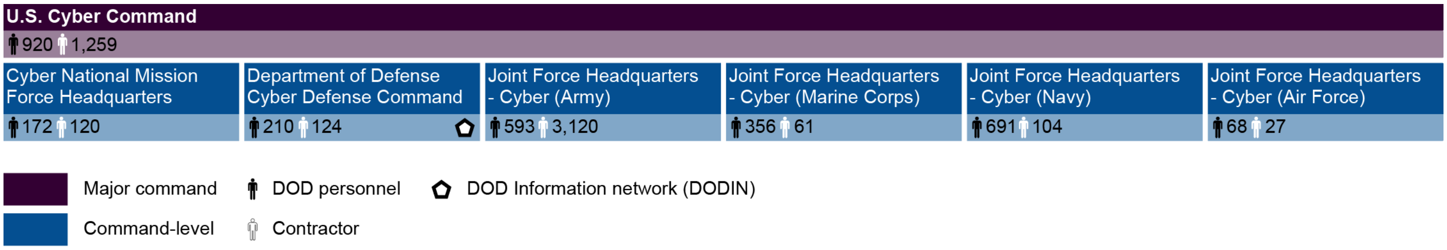
Note: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

[a] As of December 2024, the Space Force does not have any U.S. CYBERCOM-aligned organizations. According to Department of the Air Force officials, the service plans to establish a service cyber component in the middle of 2025.

CYBERCOM Authority

CYBERCOM executes authority over aligned organizations through its combatant command authority. Operational control for CYBERCOM organizations generally flows through the commander of CYBERCOM to the six operational-level organizations (i.e., Cyber National Mission Force Headquarters, DOD Cyber Defense Command, and the four Joint Force Headquarters-Cyber commands), as shown in figure 7 below. Administrative control generally flows down from the secretary of the military service through one of its respective major commands.

Figure 7: U.S. Cyber Command Organizational Construct


U.S. Cyber Command
920 1,259
Cyber National Mission Force Headquarters
172 120
Department of Defense Cyber Defense Command
210 124
Joint Force Headquarters - Cyber (Army)
593 3,120
Joint Force Headquarters - Cyber (Marine Corps)
356 61
Joint Force Headquarters - Cyber (Navy)
691 104
Joint Force Headquarters - Cyber (Air Force)
68 27
Major command
Command-level
DOD personnel
Contractor
DOD Information network (DODIN)

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Since the commanders of the Joint Force Headquarters commands also concurrently serve as the commander of their respective service cyber components (and other service commands), the personnel and contractors associated with these "multi-hatted" commands are included in these numbers.

Cyber Mission Force (CMF)

At the tactical level, the CMF conducts key cyberspace operations missions. According to the commander of CYBERCOM, DOD had 133 CMF teams and plans to increase the number of teams by at least 14 in the coming years.[1]

The CMF is generally organized into the following three elements:

- Cyber Protection Force conducts cyberspace operations for internal defense of the DOD network. The Cyber Protection Force consists of Cyber Protection Teams that are organized, trained, and equipped to defend assigned cyberspace in coordination with and in support of system operators, local defenders, cybersecurity service providers, and users.
- Cyber National Mission Force conducts cyberspace operations to defeat cyber threats to the DOD network and the nation. The force comprises various numbered national mission teams, associated

[1] We did not count the 133 CMF teams as individual organizations within this report since the teams are smaller than the unit of measurement we used (i.e., battalion- or squadron-level).

national support teams, and national Cyber Protection Teams focused on defense of non-DOD network cyberspace.

- Cyber Combat Mission Force conducts cyberspace operations to support the missions, plans, and priorities of the combatant commanders. The force comprises various numbered combat mission teams and associated combat support teams.

The total number of personnel assigned to these teams are identified in table 4 below.

Table 4: Number of Personnel and Contractors in Cyber Mission Force Teams

Service	Number of personnel	Number of contractors
Army	1,555	0
Marine Corps	504	38
Navy	1,601	2
Air Force	1,453	47

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

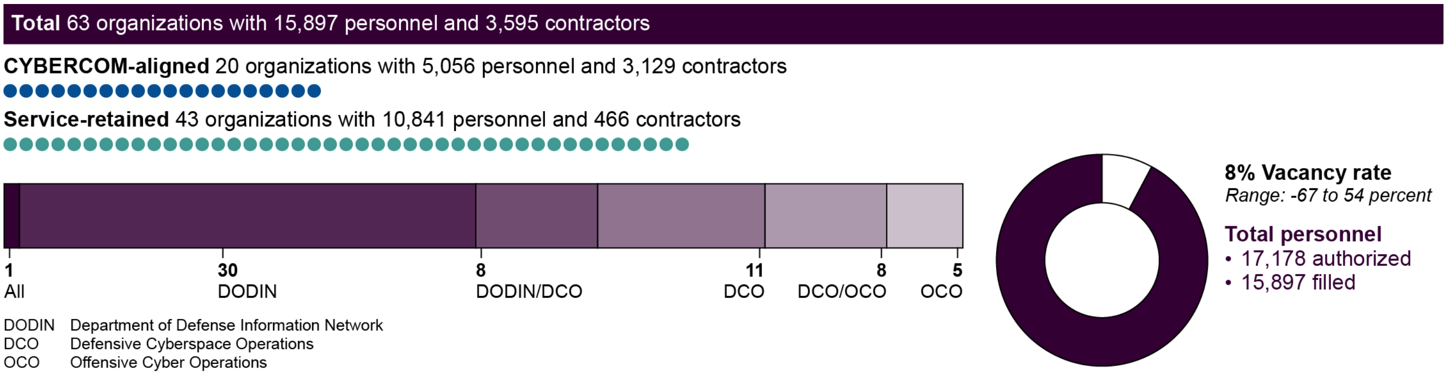
The number of Cyber Mission Force personnel and contractors depicted in this table are also included in the respective appendixes associated with each of the services (i.e., appendixes III-VII).

Appendix III: Army Cyberspace Operations

Source: U.S. Army. | GAO-25-107121

According to information that Army organizations provided us, the service has 63 organizations (consisting of 15,897 personnel and 3,595 contractors) that conduct cyberspace operations, as shown in figure 8.

Figure 8: Number of Army Organizations Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

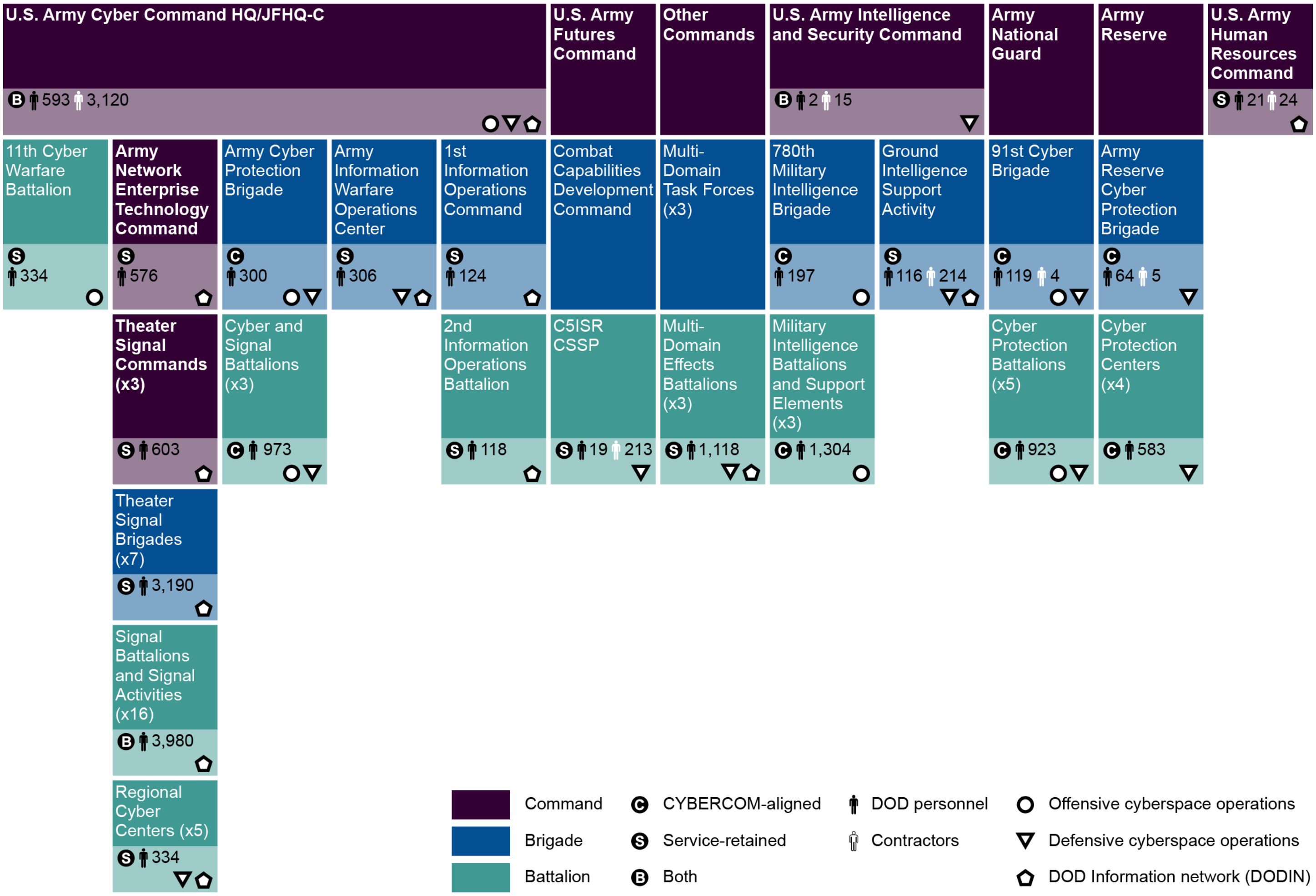
In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractors who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not to conduct cyberspace operations. We did not include these individuals within the scope of this report because DOD did not have a way to identify these individuals consistently and reliably.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -67 percent vacancy rate means that an organization conducting cyberspace operations reported having more personnel than authorized (i.e., the organization reported having only 86 authorized billets but, at the same time, reported having 144 filled cyberspace operations billets). Conversely, a 54 percent vacancy rate means that an organization conducting cyberspace operations reported having filled less than half the personnel authorized (i.e., the organization reported having 523 authorized cyberspace operations billets, but only 239 of those billets were filled).

Army Organizations and Personnel Conducting Cyberspace Operations

Army organizations that conduct cyberspace operations are organizationally aligned across seven major commands and are either aligned with U.S. Cyber Command (CYBERCOM) or retained by the Army, as shown in figure 9 below.

Figure 9: Army Organizations and Associated Personnel That Conduct Cyberspace Operations


U.S. Army Cyber Command HQ/JFHQ-C
B 593 3,120
U.S. Army Futures Command
Other Commands
U.S. Army Intelligence and Security Command
B 2 15
Army National Guard
Army Reserve
U.S. Army Human Resources Command
S 21 24
11th Cyber Warfare Battalion
S 334
Army Network Enterprise Technology Command
S 576
Army Cyber Protection Brigade
C 300
Army Information Warfare Operations Center
S 306
1st Information Operations Command
S 124
Combat Capabilities Development Command
Multi-Domain Task Forces (x3)
780th Military Intelligence Brigade
C 197
Ground Intelligence Support Activity
S 116 214
91st Cyber Brigade
C 119 4
Army Reserve Cyber Protection Brigade
C 64 5
Theater Signal Commands (x3)
S 603
Cyber and Signal Battalions (x3)
C 973
2nd Information Operations Battalion
S 118
C5ISR CSSP
S 19 213
Multi-Domain Effects Battalions (x3)
S 1,118
Military Intelligence Battalions and Support Elements (x3)
C 1,304
Cyber Protection Battalions (x5)
C 923
Cyber Protection Centers (x4)
C 583
Theater Signal Brigades (x7)
S 3,190
Signal Battalions and Signal Activities (x16)
B 3,980
Regional Cyber Centers (x5)
S 334
Command
Brigade
Battalion
C CYBERCOM-aligned
S Service-retained
B Both
DOD personnel
Contractors
○ Offensive cyberspace operations
▽ Defensive cyberspace operations
⬠ DOD Information network (DODIN)

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Organizations that do not have data in the bottom-right corner of the cell do not conduct cyberspace operations but have some level of command-and-control of Army organizations that conduct cyberspace operations.

The Army CYBERCOM-aligned organizations include higher-headquarters commands down to battalions. Within those organizations, there are smaller units (that are not counted as organizations in the CYBERCOM-aligned total for the Army. For example, within U.S. Army Cyber Command, there are personnel assigned to the three Cyberspace Operations Integrated Planning Elements located in combatant commands supported by Joint Force Headquarter-Cyber (Army). Similarly, the Army has aligned its 62 Cyber Mission Force teams within the battalions and cyber protection centers.

Service-retained organizations are spread throughout the Army. Most of these organizations are aligned under the Army Network Enterprise Technology Command and primarily provide Department of Defense Information Network (DODIN) operations. In addition to the organizations identified above, there are 60 Network Enterprise Centers subordinate to theater signal brigades (and their respective battalions). Since these centers can be subordinate to battalions, we did not count each center as an organization; however, we counted the personnel associated with these centers in the battalion totals.

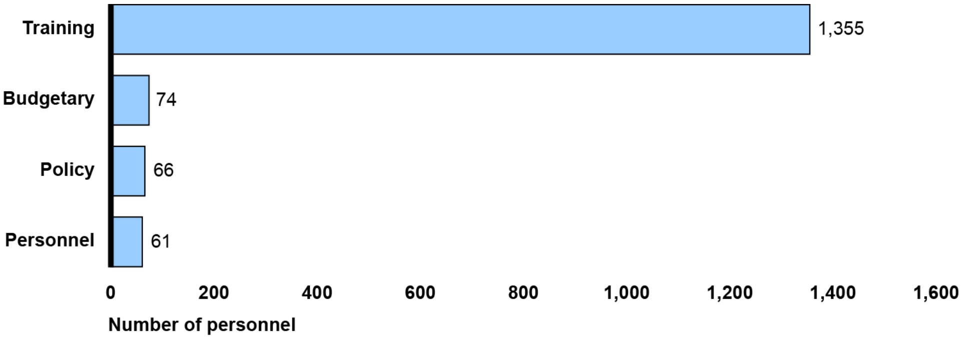
The Army has two cybersecurity service providers: (1) U.S. Army Cyber Command cybersecurity service provider, which is executed through the Army Network Enterprise Technology Command’s five regional cyber centers, and (2) U.S. Army Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center, according to Army officials.

The Army National Guard identified 347 personnel assigned to Defensive Cyber Operations Elements within each state, territory, and the District of Columbia. These units were established to support and be responsive to joint, Army, and domestic cyber requirements. We did not include these units since they are smaller than battalion-level units.

Army Organizations and Personnel Supporting Cyberspace Operations

The Army reported that 11 organizations and 1,556 personnel provide budgetary, personnel, policy, and training support for Army cyberspace operations.[1] Figure 10 shows the breakdown of Army personnel and organizations providing that support.

Figure 10: Number of Army Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Note: Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

[1] The Army also has organizations that provide other types of support such as intelligence. For example, in 2021, U.S. Army Cyber Command established a Cyber-Military Intelligence Group whose purpose is to enable U.S. Army Cyber Command to operate, defend, attack, and influence across the information dimension and cyber domain, in conflict and in competition. To do this, the group provides tailored intelligence capabilities to include the collection, analysis, and production of reports or assessments of all source intelligence and information.

Appendix IV: Navy Cyberspace Operations

Source: U.S. Navy. | GAO-25-107121

According to information that Navy organizations provided us, the service has 19 organizations (consisting of 6,741 personnel and 342 contractors) that conduct cyberspace operations, as shown in figure 11.

Figure 11: Navy Organizations and Personnel Conducting Cyberspace Operations

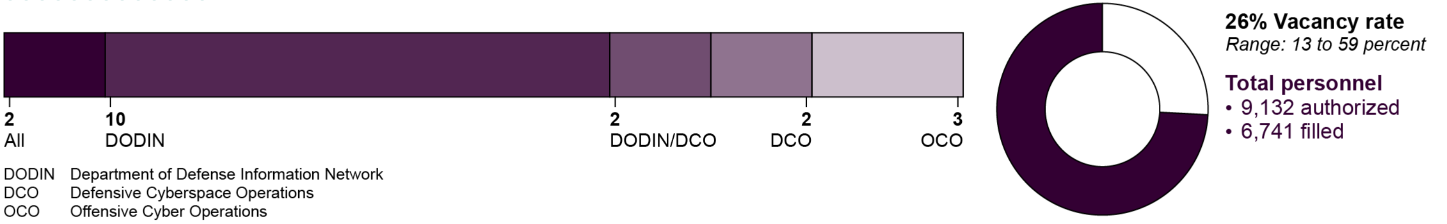
Total 19 organizations with 6,741 personnel and 342 contractors

CYBERCOM-aligned 6 organizations with 2,416 personnel and 105 contractors

●●●●●●

Service-retained 13 organizations with 4,325 personnel and 237 contractors

●●●●●●●●●●●●●



DODIN Department of Defense Information Network
DCO Defensive Cyberspace Operations
OCO Offensive Cyber Operations

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

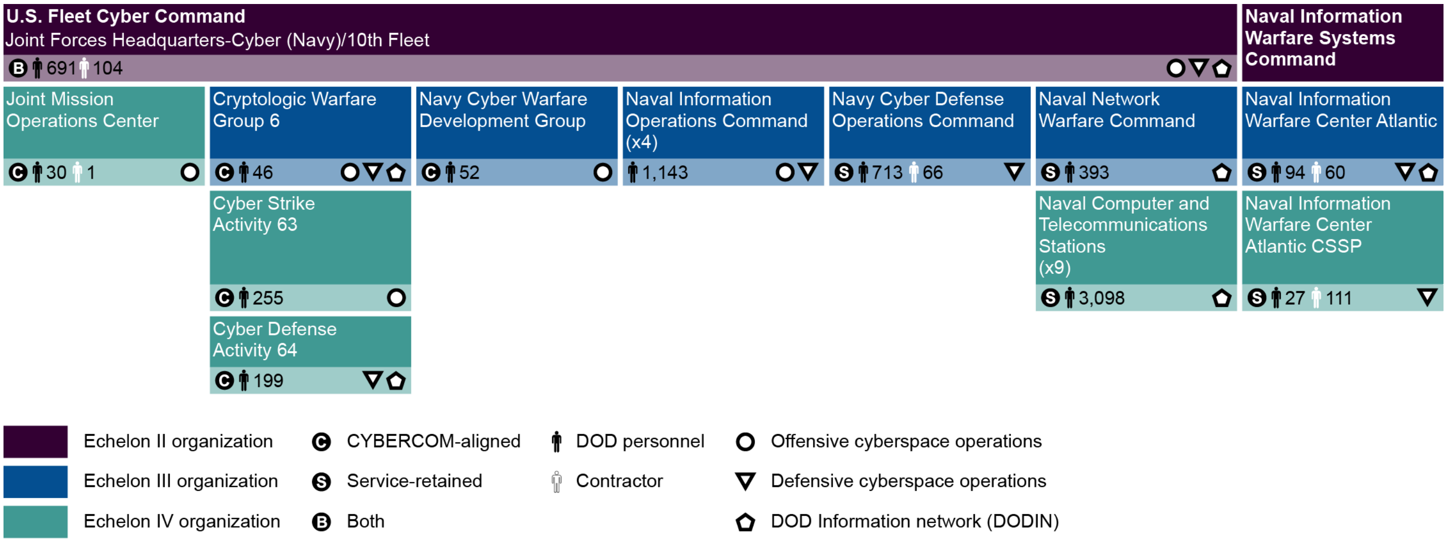
In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractors who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not to conduct cyberspace operations. For example, the Navy identified 3,038 authorized billets that conduct DODIN operations aboard naval vessels that reside in units that are not task organized to conduct cyberspace operations. We did not include these individuals within the scope of this report as DOD did not have a way to identify these individuals consistently and reliably.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a 13 to 59 percent vacancy rate means that an organization had less positions filled than authorized.

Navy Organizations and Personnel Conducting Cyberspace Operations

Most of the Navy organizations report to the “multi-hatted” commander of Fleet Cyber Command, as shown in figure 12 below.

Figure 12: Navy Organizations and Associated Personnel That Conduct Cyberspace Operations


U.S. Fleet Cyber Command
Joint Forces Headquarters-Cyber (Navy)/10th Fleet
Ⓑ 691 104
Naval Information Warfare Systems Command
Joint Mission Operations Center
Ⓒ 30 1
Cryptologic Warfare Group 6
Ⓒ 46
Navy Cyber Warfare Development Group
Ⓒ 52
Naval Information Operations Command (x4)
1,143
Navy Cyber Defense Operations Command
Ⓢ 713 66
Naval Network Warfare Command
Ⓢ 393
Naval Information Warfare Center Atlantic
Ⓢ 94 60
Cyber Strike Activity 63
Ⓒ 255
Naval Computer and Telecommunications Stations (x9)
Ⓢ 3,098
Naval Information Warfare Center Atlantic CSSP
Ⓢ 27 111
Cyber Defense Activity 64
Ⓒ 199
Echelon II organization
Echelon III organization
Echelon IV organization
Ⓒ CYBERCOM-aligned
Ⓢ Service-retained
Ⓑ Both
DOD personnel
Contractor
○ Offensive cyberspace operations
▽ Defensive cyberspace operations
⬠ DOD Information network (DODIN)

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Organizations that do not have a triangle in the bottom-right corner of the cell do not conduct cyberspace operations but have some level of command-and-control of Marine Corps organizations that conduct cyberspace operations.

The four Naval Information Operations Commands are depicted in this graphic because they provide administrative control over some Navy CMF teams. The number of personnel identified reflect the number of personnel associated with the CMF teams in this report—and not the four commands. According to Navy officials, the commands are not task-organized to conduct cyberspace operations.

Navy Cyber Defense Operations Command is a service-retained organization and includes personnel associated with one of the Navy’s cybersecurity service providers. In addition, the Navy has assigned CYBERCOM-aligned CMF teams to the command.

As reflected above, the six U.S. Cyber Command CYBERCOM-aligned organizations include higher-headquarters commands down to a unit that provides personnel to the Joint Mission Operations Center. Within those organizations, there are smaller units that are not counted as organizations in the total for the Navy. For example, within U.S. Fleet Cyber Command, there are personnel assigned to the three Cyberspace Operations Integrated Planning Elements located in combatant commands supported by Joint Force Headquarters-Cyber (Navy).

Similarly, the Navy has aligned its 40 Cyber Mission Force teams across multiple commands listed above.

The Navy-retained organizations consist of the following:

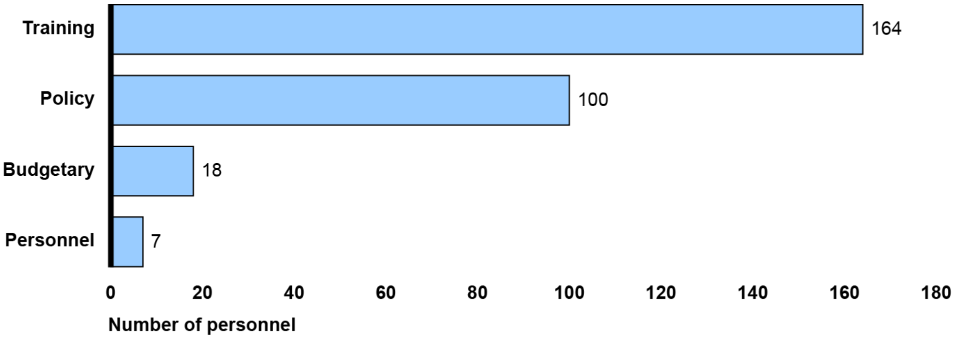
- **Navy Cyber Defense Operations Command,** which serves as the Navy's cybersecurity service provider.[1] It coordinates, monitors, and oversees the defense of Navy computer networks and systems and executes some defensive cyberspace operations.
- **Naval Network Warfare Command,** which executes tactical-level command and control to direct, operate, maintain, and secure Navy communications and network systems for the Department of Defense Information Network (DODIN) to optimize availability and security of Navy communications and network systems.
- **Naval Computer and Telecommunications Area Master Stations,** which provide command, control, communications, computers, and intelligence warfighting support to naval, joint, agency, and coalition forces afloat and ashore. They conduct DODIN cyberspace operations.
- **Naval Information Warfare Center Atlantic,** which provides information technology and electronic systems engineering, operations and support capabilities. It includes a Defense Working Capital fund nonprofit, fee-for-service organization that provides cybersecurity service provider services to other Department of Defense organizations.

Navy Organizations and Personnel Supporting Cyberspace Operations

The Navy reported that 10 organizations and 289 personnel provide policy, budgetary, and training support for Navy cyberspace operations. Figure 13 shows the breakdown of Navy personnel and organizations providing budgetary, personnel, policy, and training support.

[1] The Navy Cyber Defense Operations Command includes Cyber Mission Force personnel in addition to personnel fulfilling the command's cybersecurity service provider function.

Figure 13: Number of Navy Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

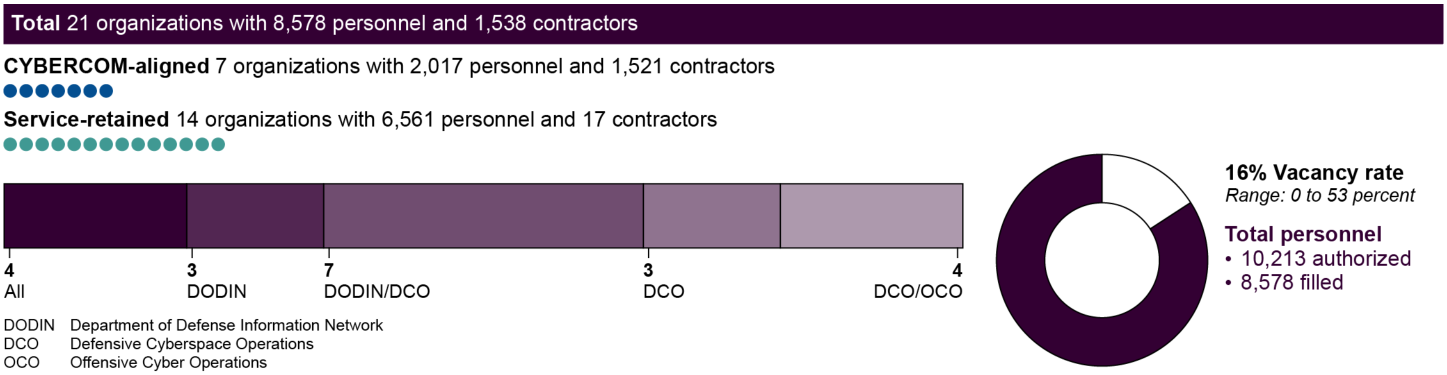
Note: Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

Appendix V: Marine Corps Cyberspace Operations

Source: U.S. Marine Corps. | GAO-25-107121

According to information that Marine Corps organizations provided us, the service has 21 organizations (consisting of 8,578 personnel and 1,538 contractors) that conduct cyberspace operations, as shown in figure 14.

Figure 14: Marine Corps Organizations and Personnel Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

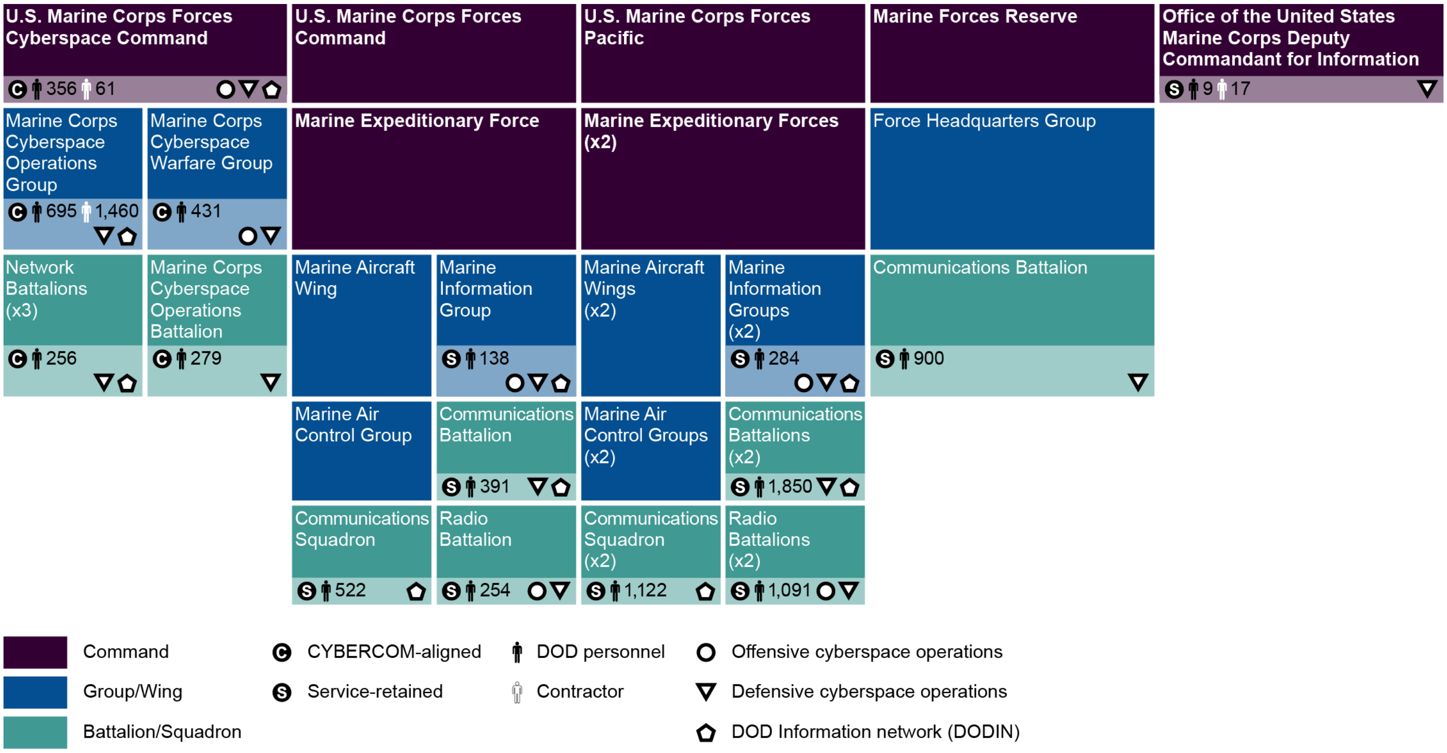
In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractors who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not to conduct cyberspace operations. For example, the Marine Corps has personnel assigned to reconnaissance battalions and logistics organizations that may conduct DODIN operations in cyberspace. We did not include these individuals within the scope of this report as DOD did not have a way to identify these individuals consistently and reliably.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a 0 percent vacancy rate means that the number of filled positions equals the number of authorized positions. A 53 percent vacancy rate means that an organization conducting cyberspace operations reported having filled less than half the personnel authorized (i.e., the organization reported having 753 authorized cyberspace operations billets, but only 356 of those billets were filled).

Marine Corps Organizations and Personnel Conducting Cyberspace Operations

As shown in figure 15 below, Marine Corps organizations are aligned under U.S. Marine Force Cyber Command or spread across the Marine Expeditionary Forces.

Figure 15: Marine Corps Organizations and Associated Personnel That Conduct Cyberspace Operations


U.S. Marine Corps Forces Cyberspace Command
Ⓒ 356 61 ○▽⬠
U.S. Marine Corps Forces Command
U.S. Marine Corps Forces Pacific
Marine Forces Reserve
Office of the United States Marine Corps Deputy Commandant for Information
Ⓢ 9 17 ▽
Marine Corps Cyberspace Operations Group
Ⓒ 695 1,460 ▽⬠
Marine Corps Cyberspace Warfare Group
Ⓒ 431 ○▽
Marine Expeditionary Force
Marine Expeditionary Forces (x2)
Force Headquarters Group
Network Battalions (x3)
Ⓒ 256 ▽⬠
Marine Corps Cyberspace Operations Battalion
Ⓒ 279 ▽
Marine Aircraft Wing
Marine Information Group
Ⓢ 138 ○▽⬠
Marine Aircraft Wings (x2)
Marine Information Groups (x2)
Ⓢ 284 ○▽⬠
Communications Battalion
Ⓢ 900 ▽
Marine Air Control Group
Communications Battalion
Ⓢ 391 ▽⬠
Marine Air Control Groups (x2)
Communications Battalions (x2)
Ⓢ 1,850 ▽⬠
Communications Squadron
Ⓢ 522 ⬠
Radio Battalion
Ⓢ 254 ○▽
Communications Squadron (x2)
Ⓢ 1,122 ⬠
Radio Battalions (x2)
Ⓢ 1,091 ○▽
Command
Group/Wing
Battalion/Squadron
Ⓒ CYBERCOM-aligned
Ⓢ Service-retained
DOD personnel
Contractor
○ Offensive cyberspace operations
▽ Defensive cyberspace operations
⬠ DOD Information network (DODIN)

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Organizations that do not have data in the bottom-right corner of the cell do not conduct cyberspace operations but have some level of command-and-control of Marine Corps organizations that conduct cyberspace operations. In responding to the draft report, U.S. Marine Corps Forces Reserve identified a communications squadron that conducts DODIN operations and defensive cyberspace operations; however, we did not include this organization and its personnel since the command did not provide us the number of authorized and filled personnel.

As reflected above, the seven U.S. Cyber Command-aligned organizations include higher-headquarters commands down to network and cyberspace operations battalions. Within those organizations, there are smaller units that are not counted as organizations in the total for the Marine Corps. For example, within U.S. Marine Forces Cyberspace Command, there are personnel assigned to a Cyberspace Operations-

Integrated Planning Element that supports U.S. Special Operations Command. Within the Marine Corps Cyberspace Warfare Group, we included personnel that are assigned to the Joint Mission Operations Center and some of the Cyber Mission Force (CMF) teams. In addition, we have included personnel associated with the remaining CMF teams within the Marine Corps Cyberspace Operations Battalion. Further, the Marine Corps Cyberspace Operations Group and its three network battalions serve as the service's cybersecurity service provider.

The Marine Corps-retained organizations that conduct cyberspace operations include:

- **Deputy Commandant of Information** that develops and supervises plans, policies, and strategy for operating in the information environment and identifies requirements in doctrine, manpower, training, education, and equipment. While this office supports organizations that conduct cyberspace operations (as noted earlier in this report), the office has two small teams—a Blue Team and a White Team—that conduct cyberspace operations.
- **Four communication battalions** that establish, maintain, and defend communication networks in support of air-ground task forces, Marine Corps component headquarters, or Joint Task Force headquarters.[1] They conduct a mix of defensive and Department of Defense Information Network (DODIN) operations.
- **Three radio battalions** that provide signals intelligence, limited cyberspace operations, and special intelligence communications support to the Marine Air Ground Task Force and Joint Forces Commander. They conduct a mix of offensive and defensive cyberspace operations.
- **Three wing communication squadrons** that provide communications support for Marine Corps aviation combat elements. They conduct DODIN cyberspace operations.

Marine Corps Organizations and Personnel Supporting Cyberspace Operations

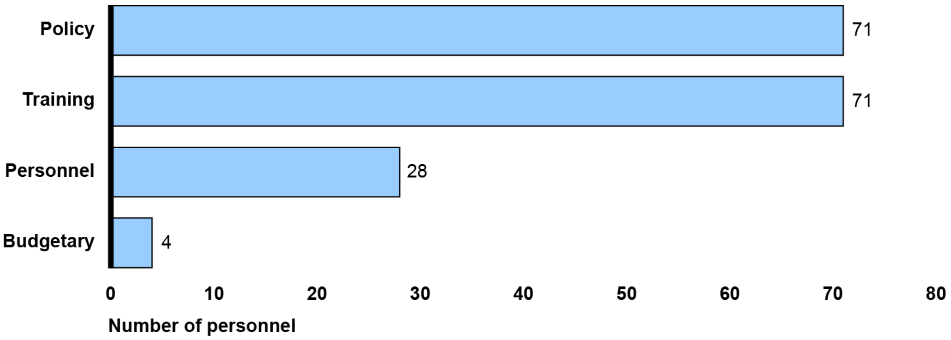
The Marine Corps reported that seven organizations with 174 personnel provide policy, personnel, budgetary, and training support for Marine Corps cyberspace operations. The Marine Corps relies on Department of Navy for budgetary, personnel, policy, and training support for cyberspace operations, but the Marine Corps Office of the Deputy

[1] In responding to the draft report, U.S. Marine Corps Forces, Pacific stated that the organization that conducted cyberspace operations subordinate to a communications battalion at the time of our review had subsequently been realigned under the III Marine Expeditionary Force Information Group.

Commandant for Information and six other Marine Corps organizations provide some support.

Figure 16 shows the breakdown of Marine Corps personnel providing budgetary, personnel, policy, and training support.

Figure 16: Number of Marine Corps Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

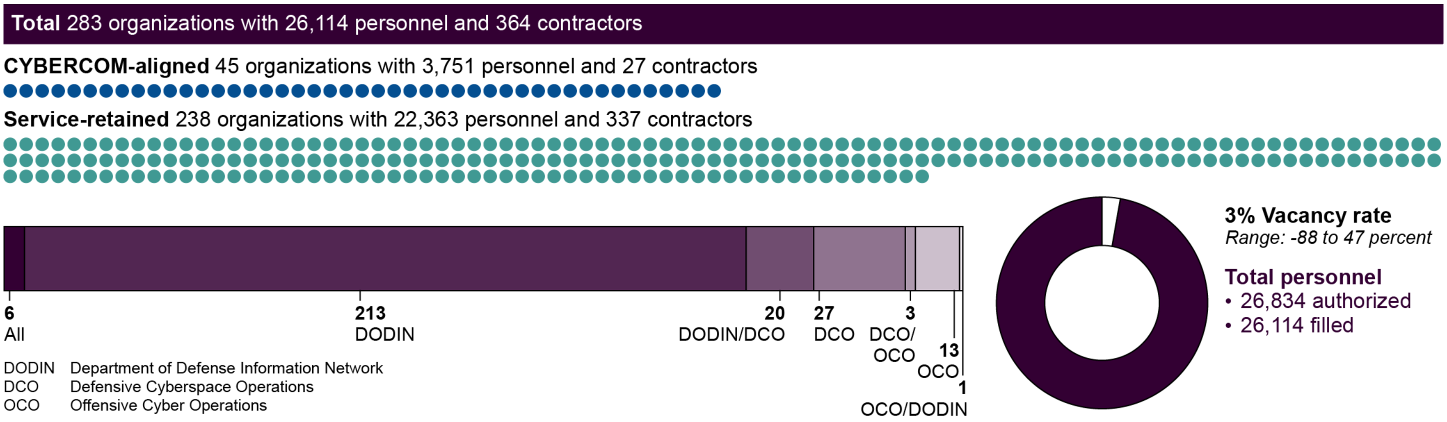
The Department of the Navy also provides support to the Marine Corps; however, to avoid double counting, we did not include Navy personnel in the Marine Corps figure totals.

Appendix VI: Air Force Cyberspace Operations

Source: U.S. Air Force. | GAO-25-107121

According to information that Air Force organizations provided us, the service has 283 organizations (consisting of 26,114 personnel and 364 contractors) that conduct cyberspace operations, as shown in figure 17 below.

Figure 17: Air Force Organizations and Personnel Conducting Cyberspace Operations



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

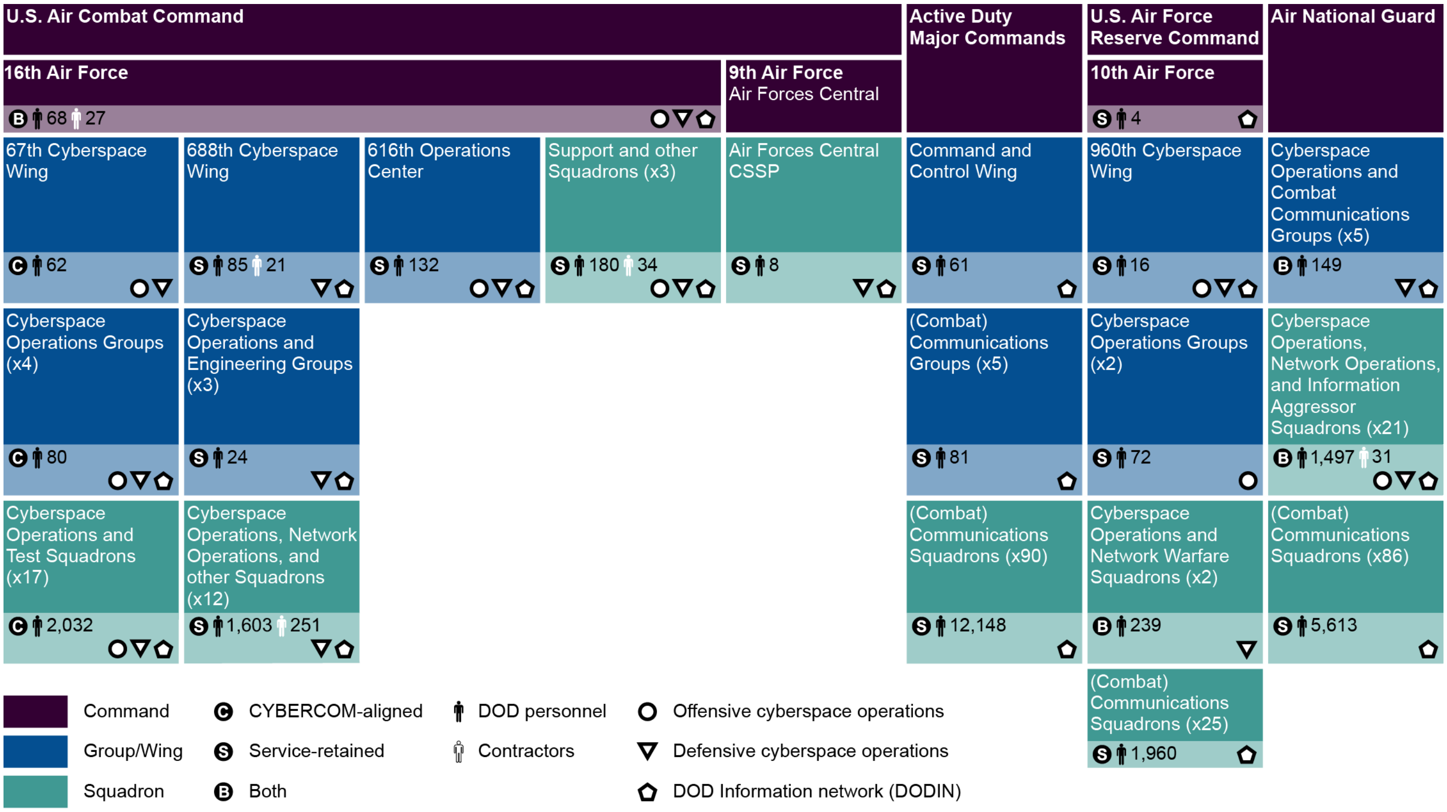
In addition to units that are established (in part or whole) for conducting cyberspace operations, there are DOD personnel and contractors who conduct cyberspace operations but are assigned to DOD organizations whose primary purpose is not to conduct cyberspace operations. For example, the Air Force may have personnel assigned within an Air Force special operations unit who conduct cyberspace operations (e.g., DODIN operations). We did not include these individuals within the scope of this report as DOD did not have a way to identify these individuals consistently and reliably.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -88 percent vacancy rate means that an organization conducting cyberspace operations reported having more personnel than authorized (i.e., the organization reported having only 43 authorized billets but, at the same time, reported having 81 filled cyberspace operations billets). Conversely, a 47 percent vacancy rate means that an organization conducting cyberspace operations reported having filled about half the personnel authorized (i.e., the organization reported having 15 authorized cyberspace operations billets, but only eight of those billets were filled).

Air Force Organizations and Personnel Conducting Cyberspace Operations

As shown in figure 18 below, Air Force organizations are spread across a multitude of major commands and down to hundreds of cyberspace operations squadrons.

Figure 18: Air Force Organizations and Associated Personnel That Conduct Cyberspace Operations


U.S. Air Combat Command
Active Duty Major Commands
U.S. Air Force Reserve Command
Air National Guard
16th Air Force
B 68 27 ○ ▼ ⬠
9th Air Force Air Forces Central
10th Air Force
S 4 ⬠
67th Cyberspace Wing
C 62 ○ ▼
688th Cyberspace Wing
S 85 21 ▼ ⬠
616th Operations Center
S 132 ○ ▼ ⬠
Support and other Squadrons (x3)
S 180 34 ○ ▼ ⬠
Air Forces Central CSSP
S 8 ▼ ⬠
Command and Control Wing
S 61 ⬠
960th Cyberspace Wing
S 16 ○ ▼ ⬠
Cyberspace Operations and Combat Communications Groups (x5)
B 149 ▼ ⬠
Cyberspace Operations Groups (x4)
C 80 ○ ▼ ⬠
Cyberspace Operations and Engineering Groups (x3)
S 24 ▼ ⬠
(Combat) Communications Groups (x5)
S 81 ⬠
Cyberspace Operations Groups (x2)
S 72 ○
Cyberspace Operations, Network Operations, and Information Aggressor Squadrons (x21)
B 1,497 31 ○ ▼ ⬠
Cyberspace Operations and Test Squadrons (x17)
C 2,032 ○ ▼ ⬠
Cyberspace Operations, Network Operations, and other Squadrons (x12)
S 1,603 251 ▼ ⬠
(Combat) Communications Squadrons (x90)
S 12,148 ⬠
Cyberspace Operations and Network Warfare Squadrons (x2)
B 239 ▼
(Combat) Communications Squadrons (x86)
S 5,613 ⬠
(Combat) Communications Squadrons (x25)
S 1,960 ⬠
Command
Group/Wing
Squadron
C CYBERCOM-aligned
S Service-retained
B Both
DOD personnel
Contractors
○ Offensive cyberspace operations
▼ Defensive cyberspace operations
⬠ DOD Information network (DODIN)

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel are defined as military service members and civilian employees working in DOD.

Organizations that do not have a triangle in the bottom-right corner of the cell do not conduct cyberspace operations but have some level of command-and-control of Air Force organizations that conduct cyberspace operations.

The Air Force has 90 (combat) communications squadrons, five (combat) communications groups, and one wing that conduct DODIN operations across the service's eight active-duty major commands. To manage the width of this figure, we depicted all active duty (combat) communications (and related Air Force organizations) in this one column. One of these combat communications groups and four of the (combat) communications squadrons are organizationally aligned under the 688th Cyberspace Wing and 616th Operations Center.

The 45 U.S. Cyber Command-aligned organizations include higher-headquarters commands down to cyberspace operations squadrons. Within those organizations, there are smaller units that are not counted as organizations in the total for the Air Force. For example, within Air Forces Cyber, there are personnel assigned to the four Cyberspace Operations Integrated Planning Elements located in combatant commands supported by Joint Force Headquarter-Cyber (Air Force). Similarly, the Air Force has aligned its 42 Cyber Mission Force teams across cyberspace operations squadrons.

Air Force-retained organizations that conduct cyberspace operations include:

- **(Combat) communications units,** which conduct Department of Defense Information Network (DODIN) operations across the Air Force. Personnel in these units comprise approximately 90 percent of the personnel in service-retained units that conduct cyberspace operations.
- **688th Cyberspace Wing,** which provides intelligence and tactics, techniques, and procedures; deployable warfighter communications; engineering and installation capabilities; defensive cyber operations; and network security operations across the Air Force network. The wing's cyberspace operations personnel are spread across the wing's headquarters, cyberspace operations groups and squadrons (including operations support squadrons, (combat) communication groups and squadrons, network operations squadrons, engineering squadrons, and intelligence support squadrons).
- **10th Air Force and the 960th Cyberspace Wing,** which serve as the Air Force Reserve component's primary contribution to service cyberspace operations missions, including offensive cyberspace operations, defensive cyberspace operations, and DODIN operations.
- **616th Operations Center** operationalizes, synchronizes, and commands and controls Air Force cyber, intelligence, and information warfare capabilities to deliver strategic effects. The unit conducts offensive, defensive, and DODIN cyberspace operations.
- **700th Air Support Squadron** supports the Air Force Commander's and the Combined Forces Air Component Commander's ability to command and control air and space forces by providing command and control data backup, continuity of operations support, operational support, and the Tier 1 Help Desk.

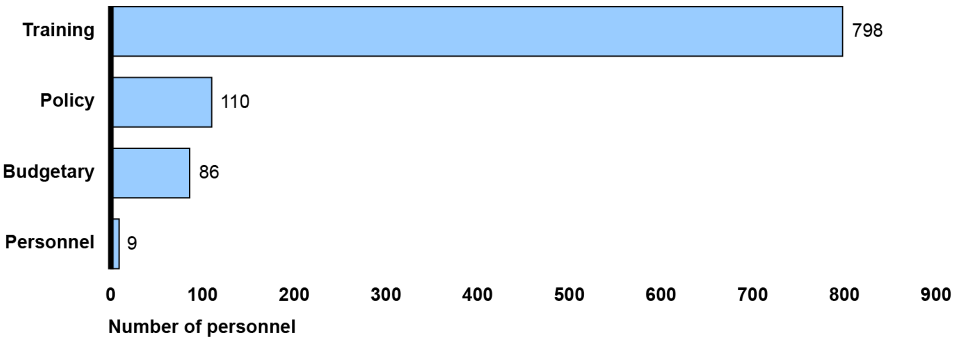
- **Cybersecurity Service Providers.** The Air Force has two components that are authorized to provide one or more cybersecurity services (such as continuous monitoring, incident handling, and DODIN user activity monitoring for the Department of Defense (DOD) Insider Threat Program) to DOD components. First, 16th Air Force has three squadrons that serve as its cybersecurity service provider. Second, U.S. Air Forces Central Command was authorized to operate as a cybersecurity service provider in 2024.

The Air Force also identified 1,490 personnel assigned to units smaller than squadrons that conduct DODIN operations. Most of these personnel (1,300) are assigned to Air National Guard communications flights. Of the remaining personnel, 170 are Air Force Reserve personnel assigned to communications flights, and 20 support an active-duty organization. We did not include these personnel in our overall count since the data were provided to us in a manner that we could not readily identify a higher-headquarters organization (i.e., squadron-level or higher) to these smaller units.

Air Force Organizations and Personnel Supporting Cyberspace Operations

The Air Force reported that 17 organizations and 1,003 personnel provide either budgetary, personnel, policy, and training support for Air Force cyberspace operations. Figure 19 shows the breakdown of Air Force personnel providing that support.

Figure 19: Number of Air Force Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Note: Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

Appendix VII: Space Force Cyberspace Operations

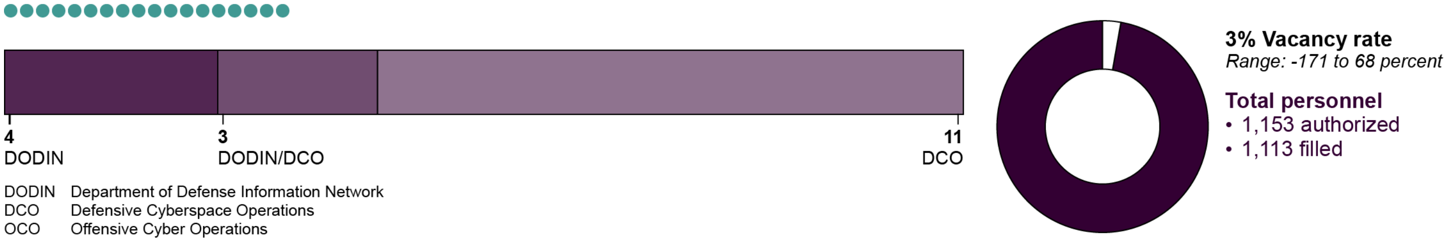
Source: U.S. Space Force. | GAO-25-107121

According to information that Space Force organizations provided us, the service has 18 organizations (consisting of 1,113 personnel and 62 contractors) that conduct or support cyberspace operations, as shown in Figure 20 below.

Figure 20: Space Force Organizations and Personnel Conducting Cyberspace Operations

Total 18 organizations with 1,113 personnel and 62 contractors

Service-retained 18 organizations with 1,113 personnel and 62 contractors



DODIN	Department of Defense Information Network
DCO	Defensive Cyberspace Operations
OCO	Offensive Cyber Operations

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

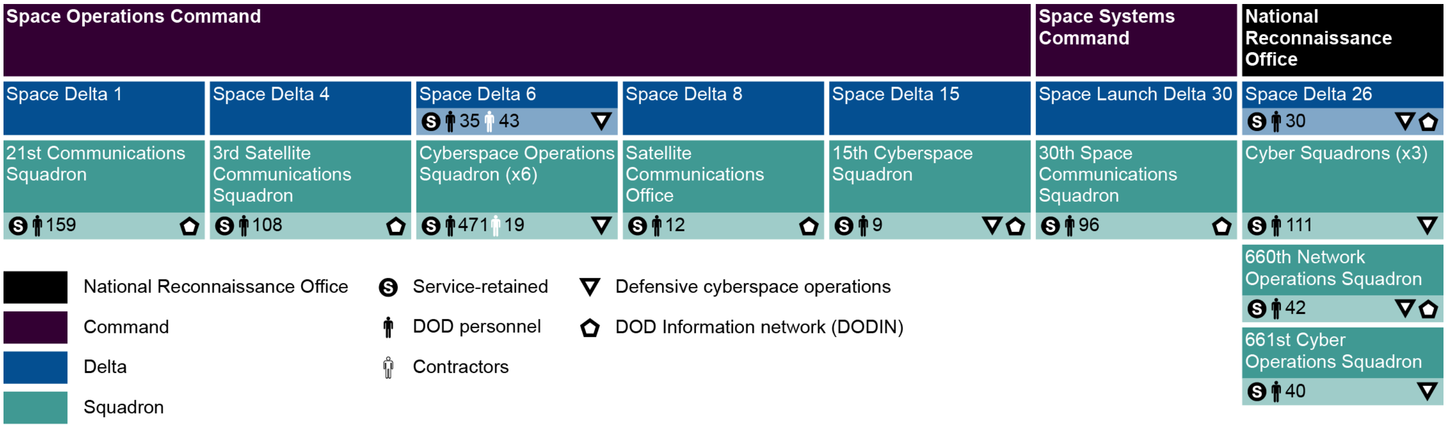
Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Our totals for personnel conducting cyberspace operations only includes filled positions. We used unfilled positions to determine how many authorized positions are vacant. Accordingly, the vacancy rate reflects the percentage of authorized billets that do not have a military service member or civilian employee filling that billet. For the purposes of the figure above, a -171 percent vacancy rate means that an organization conducting cyberspace operations reported having more than twice as many personnel than authorized (i.e., the organization reported having only 34 authorized billets but, at the same time, reported having 92 filled cyberspace operations billets). Conversely, a 68 percent vacancy rate means that an organization conducting cyberspace operations reported having filled only one-third of the personnel authorized (i.e., the organization reported having 37 authorized cyberspace operations billets, but only 12 of those billets were filled).

Space Force Organizations and Personnel Conducting Cyberspace Operations

As shown in figure 21 below, the Space Force is different than the other military services in that it: (1) does not have a service cyber component or any U.S. Cyber Command-aligned organizations and (2) does not conduct offensive cyberspace operations.[1]

Figure 21: Space Force Organizations and Associated Personnel That Conduct Cyberspace Operations



Space Operations Command					Space Systems Command	National Reconnaissance Office
Space Delta 1	Space Delta 4	Space Delta 6	Space Delta 8	Space Delta 15	Space Launch Delta 30	Space Delta 26
		Ⓢ 🧍35 👤43 ▽				Ⓢ 🧍30 ▽ ⬠
21st Communications Squadron	3rd Satellite Communications Squadron	Cyberspace Operations Squadron (x6)	Satellite Communications Office	15th Cyberspace Squadron	30th Space Communications Squadron	Cyber Squadrons (x3)
Ⓢ 🧍159 ⬠	Ⓢ 🧍108 ⬠	Ⓢ 🧍471 👤19 ▽	Ⓢ 🧍12 ⬠	Ⓢ 🧍9 ▽ ⬠	Ⓢ 🧍96 ⬠	Ⓢ 🧍111 ▽
						660th Network Operations Squadron
						Ⓢ 🧍42 ▽ ⬠
						661st Cyber Operations Squadron
						Ⓢ 🧍40 ▽

⬛	National Reconnaissance Office	Ⓢ	Service-retained	▽	Defensive cyberspace operations
🟪	Command	🧍	DOD personnel	⬠	DOD Information network (DODIN)
🟦	Delta	👤	Contractors		
🟩	Squadron				

Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Notes: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

Organizations that do not have a triangle in the bottom-right corner of the cell do not conduct cyberspace operations but have some level of command-and-control of Space Force organizations that conduct cyberspace operations.

Delta 26 is detailed to the National Reconnaissance Office but consists of U.S. Space Force units and personnel.

Since the service does not have a service cyber component, the highest-ranking organization that conducts cyberspace operations is the Space Force delta—a command that combines the wing and group command echelons found in the Air Force. The Space Force has two delta commands that conduct cyberspace operations:

- **Space Delta 6.** Space Delta 6's mission is to assure U.S. access to space through operations of the Satellite Control Network and to conduct cyberspace operations to defend Space Force space systems from adversarial attack. In addition, Delta 6 serves as the service's cybersecurity service provider.
- **Space Delta 26.** Space Delta 26 conducts defensive and Department of Defense information network cyberspace operations for the National Reconnaissance Office.

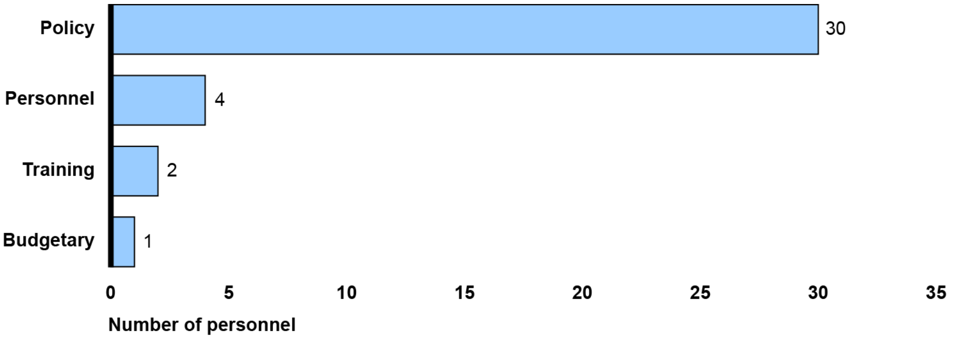
[1] According to Space Force officials, the service plans to establish a service cyber component in the middle of 2025.

Operational control for Space Force organizations conducting cyberspace operations generally flows through the Chief of Space Operations. Administrative control generally flows down from the Secretary of the Air Force through the Chief of Space Operations.

Space Force Organizations and Personnel Supporting Cyberspace Operations

The Space Force reported that four organizations with 37 personnel provide policy, personnel, budgetary, and training support for Space Force cyberspace operations. The Space Force primarily relies on the Department of the Air Force for budgetary, personnel, policy, and training support for cyberspace for operations; however, four Space Force organizations—Office of the Chief Operating Officer, Office of the Chief Technology and Innovation Officer, Space Operations Command, and Space Training and Readiness Command—also provide in-house support.[2] Figure 22 shows the breakdown of Space Force personnel and organizations providing budgetary, personnel, policy, and training support.

Figure 22: Number of Space Force Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Note: Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

The Department of the Air Force also provides support to Space Force; however, to avoid double counting, we did not include Air Force personnel in the Space Force figure totals.

[2] According to Space Force officials, the Space Force Chief Technology and Innovation Officer office was disestablished in early 2025, and the personnel in the office were assigned to the Space Force cyber and communications (S6) office.

Appendix VIII: Cybersecurity Service Provider (CSSP) Cyberspace Operations

Source: Gorodenkoff/stock.adobe.com. | GAO-25-107121

Department of Defense (DOD) Manual 8530.01 requires every DOD component to designate a component-level organization to coordinate, direct, and manage network operations and cybersecurity activities. These organizations—known as CSSPs—serve as the focal point for implementing and conducting component-wide cybersecurity activities for DOD Information Network (DODIN) operations and defensive cyber operations. CSSPs provide cybersecurity services (such as continuous monitoring, incident handling, and the insider threat process, among other services) to DOD components.

CSSPs Conduct Cyberspace Operations

As of December 2024, there are 23 DOD CSSPs authorized to operate.[1] The number of personnel assigned to two of the CSSPs are classified, but the other 21 CSSPs have 3,203 employees and four contractor personnel that conduct cyberspace operations.

Unlike other DOD organizations that conduct cyberspace operations, CSSPs have more contractor personnel than employees conducting operations across all organizations.

CSSPs can either (1) conduct operations within their own components or (2) provide services externally for other DOD components, as shown in table 5.

[1] DOD components that wish to provide cybersecurity service provider services must be authorized to operate by the command of U.S. Cyber Command every 3 years.

Table 5: Department of Defense (DOD) Cybersecurity Service Providers (CSSP)

	Type of cyberspace operation				
CSSP	Defensive cyberspace operations	DOD Information Network operations	Provides services externally	Number of employees	Number of contractors
1. 16th Air Force[a]	Yes	Yes	No	323	103
2. U.S Air Forces Central[a]	Yes	Yes	No	8	0
3. U.S. Army Cyber Command[a]	Yes	Yes	No	334	0
4. Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center[a]	Yes	No	Yes	19	213
5. Coast Guard Cyber Command[b]	Yes	Yes	No	231	68
6. Defense Advanced Research Projects Agency	Yes	Yes	No	1	80
7. Defense Finance and Accounting Service	Yes	No	No	20	18
8. Defense Information Systems Agency	Yes	No	Yes	133	498
9. Defense Intelligence Agency	Yes	No	No	19	42
10. Defense Logistics Agency	Yes	No	No	65	62
11. Defense Threat Reduction Agency	Yes	No	No	4	28
12. High Performance Computing Modernization Program	Yes	No	Yes	15	60
13. Marine Corps Forces Cyberspace Commanda	Yes	Yes	No	951	1,460
14. Missile Defense Agency	Yes	Yes	No	9	48
15. National Geospatial Intelligence Agency	Yes	No	No	29	130
16. National Reconnaissance Office	Yes	Yes	No	68	598
17. National Security Agency[c]					
18. Navy Cyber Defense Operations Commanda	Yes	No	No	713	66
19. Navy Information Warfare Center Atlantic[a]	Yes	No	Yes	27	111
20. U.S. Space Force[a]	Yes	No	No	35	43
21. U.S. Special Operations Command[c]					
22. U.S. Strategic Command	Yes	Yes	No	190	315
23. U.S. Transportation Command	Yes	Yes	No	9	40

Source: GAO analysis of DOD cyberspace operations information. | GAO-25-107121

Note: For the purposes of this report, DOD personnel is defined as military service members and civilian employees working in DOD.

[a]The number of personnel and contractors associated with service CSSPs are also included in the respective service's profile pages (see appendixes III-VII).

[b]We included the Coast Guard CSSP in this assessment since the service operates and defends a segment of the Department of Defense Information Network.

[c]The number of personnel and contactors associated with the National Security Agency and Special Operations Command are classified. Therefore, they are not included in this unclassified report.

CSSP Command and Control

Each CSSP operates under the authority of at least two separate organizations. First, CSSPs operate under the operational control and administrative control of the respective organization's leadership.[2] This leadership could be the agency's Chief Information Officer or Chief Information Security Officer, a directorate head, or a higher-headquarter military command. For example, the

- Defense Threat Reduction Agency CSSP reports to the agency's Chief Information Officer, according to Defense Threat Reduction Agency officials.
- Defense Advanced Research Projects Agency CSSP reports to the director of the agency's Information Technology Directorate.
- Service military units that serve as CSSPs for their respective services report to higher headquarter military commands.
- Three CSSPs located within a combatant command (Special Operations Command, Strategic Command, and Transportation Command) report to the head of their respective J6 directorates.

Second, CSSPs provide reporting and information to the DOD Cyber Defense Command. DOD Cyber Defense Command possesses Directive Authority for Cyberspace Operations, which provides the standing authority to direct the tactical execution of global cyberspace security, operations, and defensive actions by issuing binding orders to all elements of the DODIN.

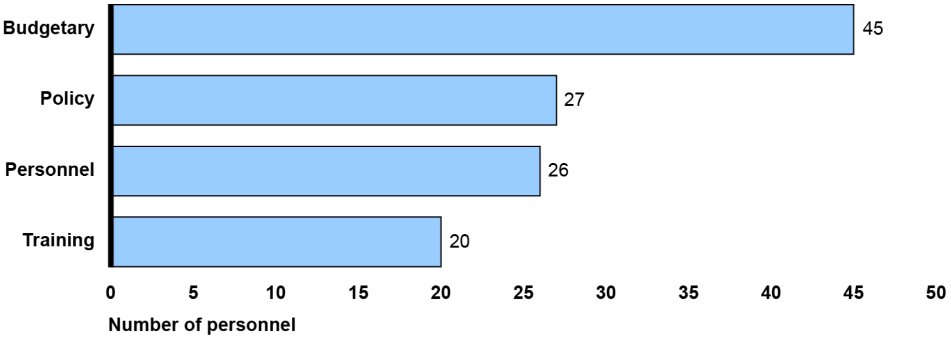
Personnel Supporting CSSP Cyberspace Operations

The non-service CSSP's receive budgetary, personnel, policy, and training support from organizations within their component. In total, according to data provided by DOD, 118 personnel provide support for CSSP cyberspace operations.[3] Figure 23 shows a comparison of the number of personnel providing these types of support for CSSP cyberspace operations.

[2] Operational control is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Administrative control is the authority necessary to fulfill military department Title 10 responsibilities for administration, support, and organizing, training and equipping military forces.

[3] This number does not include personnel providing support to service component CSSPs. Information about the services is identified in appendixes II-VII.

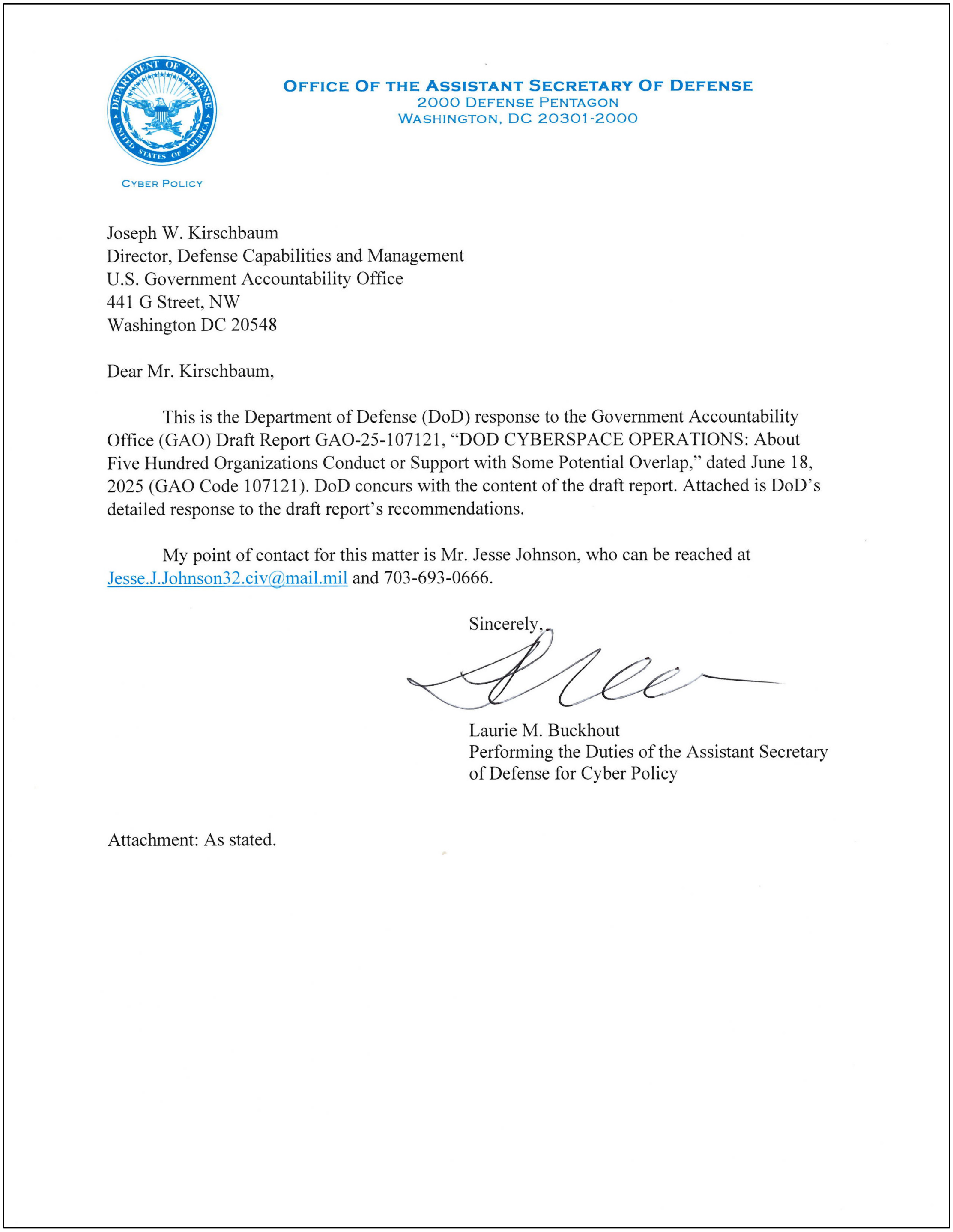
Figure 23: Number of Cybersecurity Service Provide (CSSP) Military and Civilian Personnel Providing Budgetary, Personnel, Policy, and Training Support



Source: GAO analysis of Department of Defense (DOD) cyberspace operations information. | GAO-25-107121

Note: Support personnel can work in more than one support area, so to avoid overcounting, we asked organizations to report their primary work area.

Appendix IX: Comments from the Department of Defense



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000

CYBER POLICY

Joseph W. Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Kirschbaum,

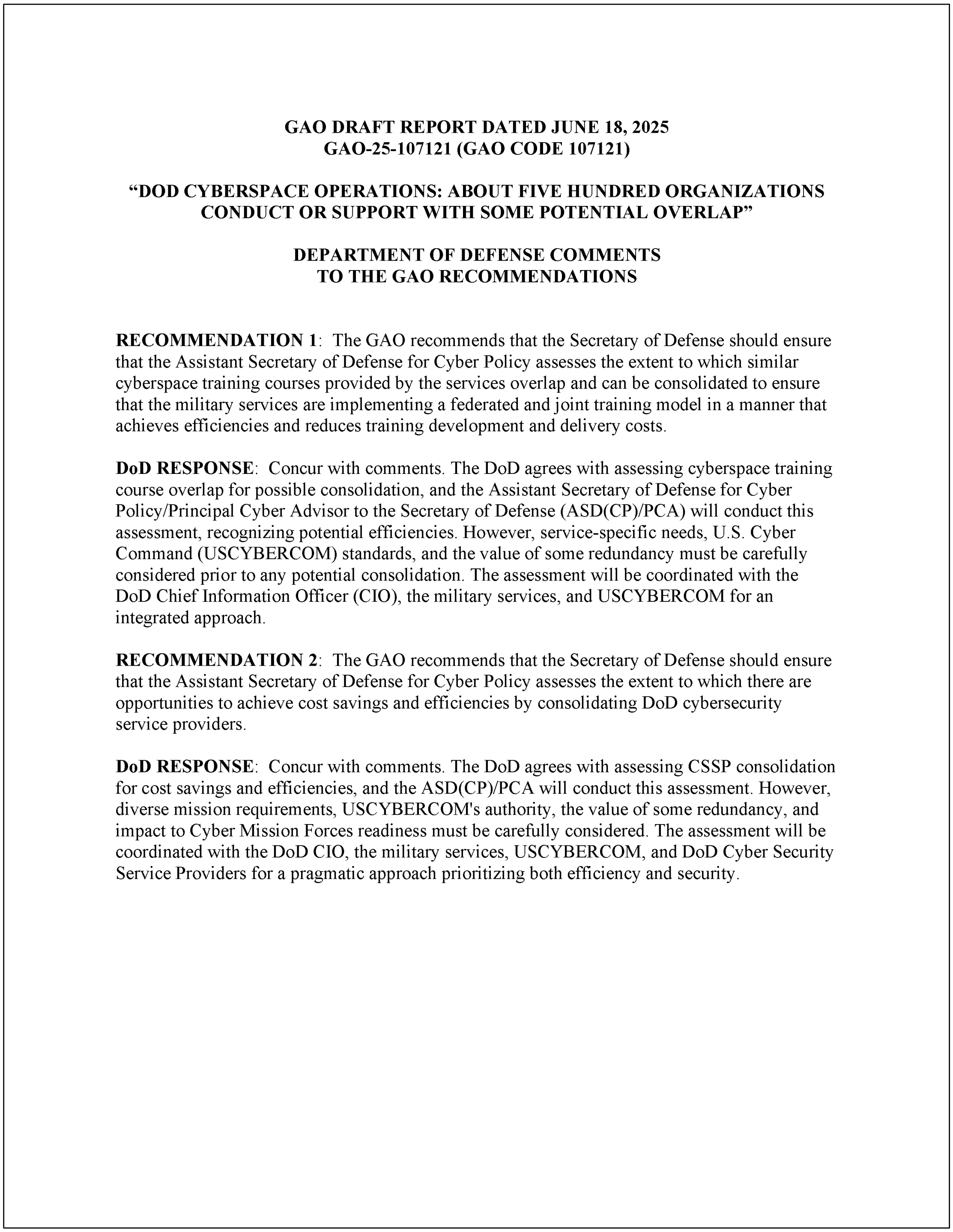
This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) Draft Report GAO-25-107121, "DOD CYBERSPACE OPERATIONS: About Five Hundred Organizations Conduct or Support with Some Potential Overlap," dated June 18, 2025 (GAO Code 107121). DoD concurs with the content of the draft report. Attached is DoD's detailed response to the draft report's recommendations.

My point of contact for this matter is Mr. Jesse Johnson, who can be reached at Jesse.J.Johnson32.civ@mail.mil and 703-693-0666.

Sincerely,

Laurie M. Buckhout
Performing the Duties of the Assistant Secretary
of Defense for Cyber Policy

Attachment: As stated.



GAO DRAFT REPORT DATED JUNE 18, 2025
GAO-25-107121 (GAO CODE 107121)

“DOD CYBERSPACE OPERATIONS: ABOUT FIVE HUNDRED ORGANIZATIONS CONDUCT OR SUPPORT WITH SOME POTENTIAL OVERLAP”

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the Assistant Secretary of Defense for Cyber Policy assesses the extent to which similar cyberspace training courses provided by the services overlap and can be consolidated to ensure that the military services are implementing a federated and joint training model in a manner that achieves efficiencies and reduces training development and delivery costs.

DoD RESPONSE: Concur with comments. The DoD agrees with assessing cyberspace training course overlap for possible consolidation, and the Assistant Secretary of Defense for Cyber Policy/Principal Cyber Advisor to the Secretary of Defense (ASD(CP)/PCA) will conduct this assessment, recognizing potential efficiencies. However, service-specific needs, U.S. Cyber Command (USCYBERCOM) standards, and the value of some redundancy must be carefully considered prior to any potential consolidation. The assessment will be coordinated with the DoD Chief Information Officer (CIO), the military services, and USCYBERCOM for an integrated approach.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that the Assistant Secretary of Defense for Cyber Policy assesses the extent to which there are opportunities to achieve cost savings and efficiencies by consolidating DoD cybersecurity service providers.

DoD RESPONSE: Concur with comments. The DoD agrees with assessing CSSP consolidation for cost savings and efficiencies, and the ASD(CP)/PCA will conduct this assessment. However, diverse mission requirements, USCYBERCOM's authority, the value of some redundancy, and impact to Cyber Mission Forces readiness must be carefully considered. The assessment will be coordinated with the DoD CIO, the military services, USCYBERCOM, and DoD Cyber Security Service Providers for a pragmatic approach prioritizing both efficiency and security.

Appendix X: GAO Contact and Staff Acknowledgments

GAO Contact

Joseph W. Kirschbaum at kirschbaumj@gao.gov

Staff Acknowledgments

In addition to the contact named above, Tommy Baril (Assistant Director), Shawn Arbogast (Analyst-in-Charge), Lucas Smith, Eli Adler, and Katherine Earle made significant contributions to this report. In addition, Sharon Ballinger, Tracy Barnes, Christopher Gezon, Elisebet Lalisan, and Michael Silver provided additional support.

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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

A. Nicole Clowers, Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us