FY2023 NDAA: Cyber Personnel Policies

October 4, 2022

Congressional Research Service
https://crsreports.congress.gov
R47270

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

FY2023 NDAA: Cyber Personnel Policies

Over the past decade, Congress, the Department of Defense (DOD), and other federal agencies have engaged in several initiatives to enhance cyber defense and warfighting capabilities and build a workforce with the technical skills needed to protect and manage digital infrastructure. The House-passed (H.R. 7900) and Senate Armed Services Committee (SASC)-reported (S. 4543) National Defense Authorization Act for Fiscal Year 2023 (FY2023 NDAA) include several provisions that relate to recruiting, retention, and career management of DOD military and civilian personnel in cyber career fields. These provisions fall into three broad categories.

- Reserve component (RC) and civilian staffing in response to cyber threats;
- Reviews of cyber personnel policies, strategy and planning; and
- Cyber-related education and training for DOD's workforce.

In legislative deliberations around the FY2023 NDAA, Congress may consider how these proposals intersect with existing federal authorities and programs related to the cyber workforce. Several of the proposed provisions would seek more clarity on DOD organization, plans, processes, and ongoing implementation of cyber workforce initiatives through periodic reports and briefings to Congress. These proposed assessments may augment or overlap with prior congressionally mandated reports or ongoing reviews. A selected list of proposed reporting requirements, deadlines, and responsible officials is provided in the Appendix of this report.

SUMMARY

R47270

October 4, 2022

Kristy N. Kamarck
Specialist in Military Manpower

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

Hibbah Kaileh
Research Assistant

Contents

Tables

Appendixes

Contacts

Background

The Department of Defense (DOD) first established the U.S. Cyber Command (USCYBERCOM, or CYBERCOM) as a subordinate command under the U.S. Strategic Command (USSTRATCOM) in 2010 in response to the growing national cyber threat. Congress elevated CYBERCOM to a unified combatant command as part of the National Defense Authorization Act for FY2017 (FY2017 NDAA).[1] The military services (Army, Navy, Air Force, Marines Corps, and Space Force) are responsible for manning, training, and equipping units assigned to CYBERCOM. These units make up the Cyber Mission Force (CMF), which executes the command's mission to direct, synchronize, and coordinate cyberspace operations in defense of U.S. national interests.[2]

Cyber Mission Force

The CMF undertakes three types of missions in cyberspace:[3]

- ***Offensive cyberspace operations*** – missions intended to project power in and through cyberspace.
- ***Defensive cyberspace operations*** – missions to preserve the ability to use cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity.
- ***Department of Defense Information Network (DODIN) operations*** – operational actions taken to secure, configure, operate, extend, maintain, and sustain DOD cyberspace and to create and preserve the confidentiality, availability, and integrity of the DODIN.[4]

The CMF's 133 teams comprise approximately 6,000 servicemembers and civilians, including reserve component personnel on active duty.[5] Reportedly, according to FY2021 budget documents, DOD expects the CMF to add 14 more teams to the existing 133 between FY2022 and FY2024, with four teams to be added in FY2022 and five in FY2023.[6] The growth is

[1] P.L. 114-328 §923; 10 U.S.C. §167b; U.S. Cyber Command, Our History, at https://www.cybercom.mil/About/History/. Cyberspace is defined by DOD in a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers. For additional information, see CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*, by Catherine A. Theohary.

[2] U.S. Army Cyber Command, "DOD Fact Sheet: Cyber Mission Force," February 10, 2020, at https://www.arcyber.army.mil/Info/Fact-Sheets/Fact-Sheet-View-Page/Article/2079594/dod-fact-sheet-cyber-mission-force/.

[3] Department of Defense Joint Publication 3-12 *Cyberspace Operations*, June 8, 2018, available at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf.

[4] Ibid. The DODIN is the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone, including owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems.

[5] For more information on the Reserve Component, see CRS In Focus IF10540, *Defense Primer: Reserve Forces*, by Lawrence Kapp.

[6] Mark Pomerleau, "Army adding more cyber teams," *FEDSCOOP*, August 17, 2022 at

expected to add about 600 people, a 10% increase, to the CMF.[7] The new CMF teams are to include both civilian and military personnel. Each military service is responsible for recruiting and training their own CMF units. CYBERCOM has reported that it is in the process of centralizing advanced cyber training, with the Army serving as the executive agent.[8]

While the CMF is CYBERCOMS's arm for operating in cyberspace as a warfighting domain, other cyber-related professionals, both military and civilian, make up the overall DOD cyber workforce. The Office of the Chief Information Officer oversees the management of DOD information technology and cybersecurity elements of the DOD cyberspace workforce.[9] Formerly known as the information assurance workforce, the cybersecurity workforce is defined in DOD Directive 8140.01 as "personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions."[10]

Cyber Excepted Service

The Cyber Excepted Service (CES) is a DOD enterprise-wide personnel system for managing defense civilians in the cyber workforce.[11] Congress established the authorities for this system as part of the FY2016 NDAA, in part to provide DOD with flexible tools to attract and retain civilians with in-demand cyber skills.[12] Prior to this law being enacted a majority of cyber positions were in the competitive service; certain existing competitive service employees were offered the opportunity to convert to CES.[13] The DOD Chief Information Officer (CIO) is responsible for developing CES policy and providing recommended policy issuances to the Undersecretary of Defense for Personnel and Readiness. According to the DOD CIO's office, there are currently 15,000 department employees in the CES, and the Department plans to expand the number of CES positions in coming years.[14]

Selected Provisions in the FY2023 NDAA

Since the creation of CYBERCOM, Congress has demonstrated concern about whether adequate resources, policies, and programs are in place to support a cyber-capable workforce. The House-

https://www.fedscoop.com/army-adding-more-cyber-teams/.

[7] C. Todd Lopez, "Cyber Mission Force Set to Add More Teams," *DOD News*, April 6, 2022, at https://www.defense.gov/News/News-Stories/Article/Article/2991699/cyber-mission-force-set-to-add-more-teams/.

[8] Testimony of U.S. Cyber Command Commander General Paul M. Nakasone, in U.S. Congress, Senate Armed Services Committee, *United States Special Operations Command and United States Cyber Command*, hearings, 117th Congress, 1st sess., March 25, 2021, at https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf.

[9] DOD doctrine uses both "cyber workforce" and "cyberspace workforce" as umbrella terms to denote DOD cyber personnel. For example, see https://dodcio.defense.gov/Cyber-Workforce/CWM.aspx.

[10] Department of Defense Directive 8140.01 *Cyberspace Workforce Management*, October 5, 2020. Available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/814001p.pdf. The term "information assurance" was removed from the DOD Dictionary of Military and Associated Terms.

[11] For more information, see CRS In Focus IF11510, *Defense Primer: Department of Defense Civilian Employees*, by Alan Ott.

[12] P.L. 114-92 §1106; 10 U.S.C. §1599f.

[13] David Knapp et al., *Employee Conversions to the Cyber Excepted Service*, RAND Corporation, Assessing Factors and Characteristics Related to Personnel Conversion Decisions, Santa Monica, CA, 2021.

[14] Justin Doubleday, *White House developing cyber workforce strategy to be more 'action oriented,'* September 9, 2022, Available at https://federalnewsnetwork.com/cybersecurity/2022/09/white-house-developing-cyber-workforce-strategy-to-be-more-action-oriented/.

passed (H.R. 7900) and Senate Armed Services Committee (SASC)-reported (S. 4543) National Defense Authorization Act for Fiscal Year 2023 (FY2023 NDAA) include several provisions that relate to recruiting, retention, and career management of DOD military and civilian personnel in cyber career fields (see **Table 1**).

Provisions in the FY2023 NDAA related to cyber personnel fall into three broad categories:

- reserve component (RC) and civilian staffing in response to cyber threats;
- reviews of cyber personnel policies, strategy and planning; and
- cyber-related education and training for DOD's workforce.

Table 1. Selected FY2023 NDAA Provisions Related to Cyber Personnel

House-passed (H.R. 7900)	SASC-Reported (S. 4543)
Reserve component (RC) and civilian staffing in response to cyber threats	
No similar provision	Section 512 would authorize the Secretary of Defense to order reserve units to active duty to respond to a significant cyber incident for a continuous period of up to 365 days.
No similar provision	Section 1112 would establish a civilian cybersecurity reserve pilot project to provide manpower to U.S. Cyber Command.
Section 1533 would require DOD to conduct a comprehensive review of the Cyber Excepted Service policies, including personnel compensation and advancement.	Section 1114 would require DOD to report annually on Cyber Excepted Service positions.
Reviews of cyber personnel policies, strategy and planning	
	Section 1606 would require a DOD study on the responsibilities of the military services for organizing, training, and presenting the total force to CYBERCOM.
Section 1531 would require DOD annual reports to be submitted with the President's budget request on CMF readiness and the adequacy of policies, plans, procedures, and the execution of manning, training, and equipping the CMF starting in FY2024.	Section 1603 would require the Secretary of Defense and the Chairman of the Joint Chiefs of Staff to develop a plan and recommendations to address CMF personnel readiness shortfalls. Section 1610 would require a review of certain cyber operations personnel policies, including recruitment, retention, professional military education, personnel data sharing, structures, and departmental guidance and processes.
Section 1503 would direct the Secretary of the Navy to establish and sustain certain Cyber Warfare career designators as well as a training pipeline and implementation plan.	Section 1625 would require the Secretary of the Navy to report on recommendations for improving cyber career paths in the Navy.
Section 1532 would require an independent review of the staffing levels of DOD's Office of the Chief Information Officer (CIO).	No similar provision
Education and Training	
Section 1535 would establish a "Hacking for National Security and Public Service Innovation Program" (H4NSPSI) to, in part, support the development and acquisition of cyber talent in the federal workforce.	No similar provision

House-passed (H.R. 7900)	SASC-Reported (S. 4543)
Section 558 would require the Secretary of Defense to establish a consortium of military and civilian education institutions to provide a forum to share information on matters of cybersecurity.	No similar provision
No similar provision	Section 1111 would establish a program to provide financial support for the pursuit of programs in disciplines related to cyber or digital technology at institutions of higher education.

Source: CRS analysis of legislation on Congress.gov.

Notes: Several provisions in the House-passed and SASC-reported bill would address other aspects of military cyber policy beyond the scope of this product, including: organizational structure, roles, and missions; cyber warfighting architecture; strategy alignment and interagency coordination; cyber innovation incentives; and foreign military cooperation.

Discussion

Reserve Component and Civilian Staffing in Response to Cyber Threats

Some experts have called for leveraging the Reserve Component (RC) to meet increased demand for cyber personnel. A 2017 RAND study found that tens of thousands of reservists either have cyber expertise or are able to easily acquire cyber-related skills through civilian-based training, and many express a desire to use these skills in the military.[15] In a March 2021 Senate Armed Services Committee Hearing, CYBERCOM Commander Paul Nakasone called the ability to bring on personnel with relevant private-sector expertise "invaluable."[16] Provisions in the SASC-reported version of the FY2023 NDAA would expand authorities for activating RC members and hiring civilians to respond to "significant cyber incidents."[17] Section 512 of the SASC-reported bill would amend 10 U.S.C. §12304 to authorize the Secretary of Defense to involuntarily activate individuals in the Selected Reserve and Individual Ready Reserve for up to 365 continuous days to respond to such events.[18] There are no similar provisions in the House bill.

[15] Isaac R. Porche III, Caolionn O'Connell, John S. Davis II, et al., *Cyber Power Potential of the Army's Reserve Component.* Santa Monica, CA: RAND Corporation, 2017, at https://www.rand.org/pubs/research_reports/RR1490.html.

[16] Testimony of U.S. Cyber Command Commander General Paul M. Nakasone, in U.S. Congress, Senate Armed Services Committee, *United States Special Operations Command and United States Cyber Command*, hearings, 117th Congress, 1st sess., March 25, 2021, at https://www.armed-services.senate.gov/imo/media/doc/Nakasone_03-25-21.pdf.

[17] Presidential Policy Directive/PPD-41 United States Cyber Incident Coordination defines a significant cyber incident as one that is "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people." July 26, 2016, at https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[18] 10 U.S.C. §12304 currently authorizes the President to involuntarily mobilize reservists for certain emergencies related to "use or threatened use of a weapon of mass destruction" or "a terrorist attack or threatened terrorist attack in the United States that results, or could result, in significant loss of life or property." For more information, see CRS Report RL30802, *Reserve Component Personnel Issues: Questions and Answers*, by Lawrence Kapp and Barbara Salazar Torreon.

Section 1112 of the SASC-reported bill would require the Secretary of the Army to establish a four-year "Civilian Cybersecurity Reserve" pilot project to augment the CYBERCOM workforce.[19] This pilot authority would allow the Army to establish criteria for selection into the Civilian Cybersecurity Reserve and would allow for noncompetitive temporary appointments of up to 50 personnel into the competitive service (under 5 U.S.C. §2102) and excepted service (under 5 U.S.C. §2103).[20]

Title 10 of the *U.S. Code* includes some existing special authorities that allow DOD to recruit, retain, and develop individuals with cyber or information technology skills. These Cyber Excepted Service (CES) authorities were intended in part to give DOD more flexibility when hiring for cyber and IT jobs.[21] While provisions in the House-passed and SASC-reported bills would not amend CES authorities, they would require review of CES policies and positions. Section 1533 of H.R. 7900 would require a comprehensive review of pay and compensation disparities between CES and the private sector, eligibility criteria for participation in CES, and whether there are limitations on the mobility and advancement of civilians in CES. Section 1114 of the SASC-reported bill would require DOD to report annually on CES positions, workforce planning, training, and other aspects of the use and effectiveness of existing authorities.

Reviews of cyber personnel policies, strategy, and planning

The House-passed and SASC-reported bills call for several assessments, reports, and briefings on the state of the cyber workforce and plans for the recruitment, retention, and career management of this force (see **Appendix** for a list of reporting requirements). Congress might consider how these provisions would build on or overlap with research and analysis efforts from prior congressionally mandated reviews, for example, the "zero-based review" (ZBR) of the cyber and information technology personnel" required section 1652 of the FY2020 NDAA (P.L. 116-92), or reports and briefings regarding cyber personnel education matters required by section 1506 of the FY2022 NDAA (P.L. 117-81) [22]

Section 1531 of the House bill would require the CYBERCOM Commander to submit a report in conjunction with the President's annual budget request to Congress[23] that evaluates the support by military departments for cyberspace operations, and CMF capability, readiness, and resourcing. This reporting requirement would go into effect in the FY2024 budget cycle. The FY2021 NDAA also delegates responsibility to the CYBERCOM commander for directly controlling and

[19] The congressionally mandated National Commission on Military, National, and Public Service recommended such a project in 2020. National Commission on Military, National, and Public Service, *Inspired to Serve*, March 2020, p. 81, at https://www.volckeralliance.org/sites/default/files/attachments/Final%20Report%20-%20National%20Commission.pdf.

[20] For more on federal civilian service see CRS Report R45635, *Categories of Federal Civil Service Employment: A Snapshot*, by Jon O. Shimabukuro and Jennifer A. Staman.

[21] P.L. 114-92 §1107; 10 U.S.C. §1599f.

[22] A *zero-based review* is defined in this context as "review in which an assessment is conducted with each item, position, or person costed anew, rather than in relation to its size or status in any previous budget." DOD reported in April 2021 that component-level ZBR reviews and recommendations were to be completed by December 2021 and reported to the Congress by June 2022. See Senate Armed Services Committee, *Statement by John Sherman, Acting Chief Information Officer for DOD Before the Senate Armed Services Committee on Cyber Workforce*, April 21, 2021; and Molly McIntosh et al., *Support to the DOD Cyber Workforce Zero-Based Review; Developing a Repeatable Process for Conducting ZBRs within DOD*, RAND Corporation, Santa Monica, CA, 2022.

[23] 31 U.S.C. §1105.

managing the planning, programming, budgeting, and execution (PPBE) of resources starting in the FY2024 budget cycle.[24]

Several proposals in the SASC-reported bill would require DOD to consider how it staffs and trains the cyber workforce and what the roles and responsibilities of the military services are in this regard. Section 1603 of the SASC-reported bill would require DOD to develop a plan to address CMF "readiness shortfalls" with recommendations for legislative action in areas, such as promotion, assignment, training, and compensation authorities. Section 1610 of the SASC-reported bill would require DOD to review and report on policies related to the CYBERCOM Commander's authority under 10 U.S.C. §167b to monitor "the promotion of cyber operation forces and coordinating with the military departments regarding the assignment, retention, training, professional military education, and special and incentive pays of cyber operation forces."[25]

Section 1606 of the SASC-reported bill would require DOD to consider a new force generation model for CYBERCOM.[26] This study would include consideration of use of the RC and nonmilitary personnel[27] to support CMF teams, along with different training models. The CYBERCOM Commander would be responsible for providing a proposed force generation plan to the Secretary of Defense no later than June 1, 2024, and the Secretary would be required to submit an implementation plan to Congress no later than June 1, 2025. This provision of the SASC-reported bill also explicitly directs the Secretary of Defense to consider whether the Navy should continue to be involved in developing and providing personnel and resources to CYBERCOM. In recent years, some observers identified the Navy as the least capable of the military services for cyberspace operations and cybersecurity.[28] The Navy is the only military branch without service-retained offensive cyber units and according to critics, lacks sufficient cyber capabilities, forces, and training.[29] Navy leadership views cyber operations as a joint endeavor, relying on other services' warfighting capabilities with support from its cryptologic warfare officers whose mission differs from that of other cyber operators.[30]

Other provisions in the House-passed and SASC-reported bill would specifically address the Navy's cyber career paths. Section 1503 of the House-passed bill would direct the Secretary of the Navy to establish and sustain a specific Cyber Warfare Operations career field for uniformed personnel, including a training pipeline and implementation plan. The Navy does not currently have a dedicated military occupational specialty (called a *designator* for officers or *rating* for enlisted members) for cyber operations. The House bill would prohibit the Navy from assigning servicemembers with non-cyber designators or ratings to a CMF after June 1, 2024. Some critics

[24] P.L. 117-81 §1507. For more on PPBE, see CRS Report R47178, *DOD Planning, Programming, Budgeting, and Execution (PPBE): Overview and Selected Issues for Congress*, by Brendan W. McGarry.

[25] 10 U.S.C. §167b.

[26] A force generation model is a structured process for providing trained personnel to meet service or joint operational needs.

[27] Section 1606 describes *nonmilitary* personnel as "civilian government employees, contracted experts, commercial partners, and domain or technology-specific experts in industry or the intelligence community."

[28] Lieutenant Commander Derek Bernsen USN, "The Navy Needs a Cyber Course Correction," *Proceedings Vol. 148/8/1,434*, U.S. Naval Institute, August 2022 available at https://www.usni.org/magazines/proceedings/2022/august/navy-needs-cyber-course-correction.

[29] Ibid.

[30] Ibid. Personnel who support cyber operations are primarily sourced from the Cryptologic Warfare (CW), Information Specialist, Intelligence and Cyber Warfare Engineer communities. The CW community is generally responsible for signals intelligence, electronic warfare, and information operations.

argue that requiring the Navy to establish a dedicated Cyber Warfare Operations career field would encourage the Navy to place a higher priority on its offensive cyber mission, while others contend that the status quo is adequate and proposed career field changes are unnecessary.[31] Section 1625 of the SASC-passed bill would not require new career designators/ratings, but would require the Secretary of the Navy to report on recommendations for improving cyber career paths in the Navy.

Education and Training of DOD's Cyber Workforce

Provisions in the FY2023 NDAA bills would seek to develop or strengthen partnerships with academic institutions and other federal agency programs to support a pipeline for a federal cyber workforce and to support continuing education and training for existing DOD uniformed and civilian personnel. These provisions could potentially augment existing DOD programs and initiatives such as

- the *Hacking for Defense* (HFD) program;
- federal grants for DOD Cyber Institute pilot programs at institutions of higher education;[32]
- the *University Consortium for Cybersecurity* (UC2);[33] and
- capacity building grants and scholarships under the Cyber Scholarship Program (CySP).[34]

Section 1535 of the House-passed bill would require DOD to establish a "Hacking for National Security and Public Service Innovation Program" (H4NSPSI) to, in part, "support the development and acquisition" of cyber talent in the federal workforce. The bill would direct the DOD-led National Security Innovation Network (NSIN) to coordinate the H4NSPSI effort with other federal agencies and academic institutions. NSIN currently sponsors a 10-16 week *Hacking for Defense* (H4D) college course that engages student teams in working on real-world national security programs.[35] Other agencies sponsor similar programs: for example, Hacking for Homeland Security (Department of Homeland Security; DHS) and Hacking for Diplomacy (Department of State).[36] Section 1535 would encourage DOD to coordinate and partner with these and other federal agency-led programs.

Section 558 of the House-passed bill would require the Secretary of Defense to establish a consortium of military and civilian education institutions to provide a forum to share information

[31] Mark Pomerleau, "House Armed Services Committee concerned with state of Navy cyber readiness," *FEDSCOOP*, July 28, 2022, at https://www.fedscoop.com/house-armed-services-committee-concerned-with-state-of-navy-cyber-readiness/.

[32] As authorized by the FY2019 NDAA (P.L. 115-232, Section 1640). DOD has established this pilot program at the six senior military colleges: Norwich University, in Northfield, Vermont; Texas A&M University, in College Station, Texas; The Citadel, in Charleston, South Carolina; Virginia Military Institute, in Lexington, Virginia; Virginia Tech, in Blacksburg, Virginia; and the University of North Georgia, in Dahlonega, Georgia. The FY2021 NDAA (P.L. 116-283 §283) amended the pilot program authority to require a report to Congress by September 30, 2021 on opportunities to report on the effectiveness of the Cyber Institutes and on opportunities to expand these to other institutions with ROTC units.

[33] As mandated by the FY2020 NDAA (P.L. 116-92, Section 1659).

[34] As authorized by 10 U.S.C. §2200b.

[35] NSIN, Hacking for Defense, at https://www.nsin.mil/hacking-for-defense/.

[36] See https://www.dhs.gov/science-and-technology/hacking-homeland-security and https://www.bmnt.com/hacking-4-diplomacy.

on matters related to cybersecurity.[37] Functions of this consortium would include sharing information on the "education of cyber mission forces." The consortium would be required to conduct annual cyberspace war games with its members. Section 558 would direct the Secretary of Defense to coordinate the efforts of this new consortium with the "Consortia of Universities to Advise Secretary of Defense on Cybersecurity Matters" previously mandated by Section 1659 of the FY2020 NDAA.[38] This consortium, called the *University Consortium for Cybersecurity* (UC2), was launched on December 7, 2021, and is led by the National Defense University College of Information and Cyberspace.[39] In deliberations around the FY2023 NDAA, Congress might consider whether Section 558 of the House bill would create a parallel consortium, or would expand the mandate of the existing consortium.

In the SASC-reported bill, Section 1111 would require the Secretary of Defense, in consultation with DHS and the Office of Personnel Management (OPM), to establish a "Department of Defense Cyber and Digital Service Academy" program to provide financial support for the pursuit of educational programs at institutions of higher education in "critical" disciplines related to cyber or digital technology. Covered disciplines would include computer-related arts and sciences, cyber-related engineering, cyber-related law and policy, applied analytics-related sciences, data management, and digital engineering, including artificial intelligence and machine learning. This program would provide up to five years of academic scholarship assistance—similar to Senior Reserve Officer Training Corps (SROTC) scholarships—to qualified students in a course of study in one of the covered disciplines.[40] Students who accept scholarship funding would incur a federal employment commitment equal to the length of the scholarship. The provision would require at least 50% of the funding authorized for this program to be directed to institutions of higher education that have used federal grant funding under DOD's Cyber Scholarship Program (CySP).[41] CySP currently provides recruitment and retention scholarship support to students and DOD personnel, along with capacity-building grants to institutions.[42]

[37] These institutions include institutes of higher education with established cybersecurity programs; military service academies; professional and joint professional military education schools under 10 U.S.C. §§2151 and 2162; and the Naval Postgraduate School.

[38] P.L. 116-92.

[39] National Defense University, College of Information and Cyberspace, The Department of Defense University Consortium for Cybersecurity Coordination Center, at https://cic.ndu.edu/UC2/.

[40] For more on SROTC, see CRS In Focus IF11235, *Defense Primer: Senior Reserve Officer Training Corps*, by Kristy N. Kamarck.

[41] This grant program is authorized by 10 U.S.C. §2200b.

[42] DOD Cyber Exchange, DOD Cyber Scholarship Program, at https://public.cyber.mil/cw/cdp/dcysp/.

Appendix. Selected Reporting Requirements

Table A-1. Selected Reporting Requirements Proposed in the FY2023 NDAA

Section	Matters to be Studied and Reported	Reporting Entity	Due Date for Report to Congress
SASC Section 1112	*Civilian Cybersecurity Reserve Pilot Project* - Number and diversity of program participants; - ethical considerations; - effectiveness in adding to Army capacity; and - evaluation of eligibility requirements.	Secretary of the Army	Implementation plan within one year and 60 days following enactment, Annual briefings
	- Evaluation of the pilot program.	Government Accountability Office (GAO)	3 years following pilot establishment
House Section 1531	*Annual reports on support by military departments for cyberspace operations* - Whether military departments are meeting CYBERCOM's validated requirements; - adequacy of military department policies, procedures, execution, and investment in - manning, training, equipping, - assignment to CMF (including assignment duration), - investment in CMF capabilities, and - cyberspace-related military occupational specialties, designators, ratings, or specialty codes; and - readiness of CMF and cyberspace operations forces.	CYBERCOM Commander	FY2024 budget request (and annually thereafter)
SASC Section 1603	*Correcting cyber mission force readiness shortfalls* - Analysis of options and a plan to increase personnel in key cyber roles, to include - number of personnel needed, - proper mix of civilian/military/contractor, - use of existing, alternate, or standardized compensation models, and - modifying career paths for consecutive assignments or multiple rotations; and - modifying promotion systems.	Secretary of Defense and Chairman of Joint Chiefs of Staff	180 days following enactment

Section	Matters to be Studied and Reported	Reporting Entity	Due Date for Report to Congress
SASC Section 1606	*Total force generation for the Cyberspace Operations Forces* - Which military services (including consideration of a separate service) should organize, train, and equip military and civilian assets for assignment to CYBERCOM; - sufficiency of accession and training models for Cyberspace Operations Forces; - whether Cyberspace Operations Forces are appropriately organized; - shortfalls in work roles and skills; - unique or training-intensive roles and plans for development and retention in those roles; - whether compensation, career management, evaluations, and training are appropriate; - use of nonmilitary and/or reserve component personnel to augment CMF teams; and - proper mix of civilian/military/contractor.	Secretary of Defense Principal Cyber Advisor and CYBERCOM Commander Secretary of Defense	Progress briefings 90 days after enactment and every 180 days thereafter Recommendations to Secretary of Defense Before June 1, 2024. Implementation plan to Congress by June 1, 2025
SASC Section 1610	*Review of certain cyber operations personnel policies* - The respective roles of the military departments and CYBERCOM with respect to: - the recruitment, retention, professional military education, and promotion of certain cyber operations personnel; - the sharing of personnel data between the military departments and CYBERCOM; and - structures, departmental guidance, and processes developed between the military departments and U.S. Special Operations Command that could be used as a model for CYBERCOM. - Findings of the Secretaries of the military departments and CYBERCOM commander with respect to the review and updates made following the report, including recommendations for legislative or administrative action.	Secretary of Defense Secretary of Defense	180 days following enactment 90 days after review is submitted
House Section 1532	*Independent review of posture and staffing levels for the office of the CIO* - Any limitations on the CIO's office imposed by staffing levels; and - composition of civilian, military, and contractor personnel assigned to the CIO's office.	Independent Review (non-DOD entity)	30 days after review complete
House Section 1533	*Comprehensive review of Cyber Excepted Service (CES)* - Structural limitations on the mobility or advancement for civilians in the CES; - pay/compensation disparities between CES and comparable private sector employees; and - eligibility criteria for participation in the CES.	DOD Chief Information Officer	30 days after review complete

Section	Matters to be Studied and Reported	Reporting Entity	Due Date for Report to Congress
SASC Section 1114	*Report on Cyber Excepted Service* - A description of the hiring and selection process for the CES; - plans for recruitment and retention in the CES; - assessment of training provided to CES supervisors; - assessment of barriers to CES participation; - assessment of implementation of CYBERCOM recruitment and retention under 10 U.S.C. §1599f; and - performance metrics including; - number of employees by occupation, grade, and level or pay band, - placement of employees by military department, agency, and component, - number of veterans hired, - number of separations by occupation, grade, and level or pay band, - number and amounts of incentives paid, and - number of employees that declined transfer to CES positions.	Secretary of Defense	One year following enactment and annually until 2028
House Section 1503	*Establishment of cyber operations designator and rating for the Navy* - Certification that the Navy has - established a separate Cyber Operations career designator, - identified responsibilities for staffing and training the career field, - established a training pipeline, - established adequate funding for training, - inventoried flag officer positions related to career field, - established an implementation plan for filling CMF positions; and - provided anticipated end-strength changes related to the new career designator.	Secretary of the Navy	One year following enactment
	- CYBERCOM verification that the Navy's report satisfies requirements.	CYBERCOM	60 days after Navy report submitted
SASC Section 1625	*Report on Recommendations from Navy Civilian Career Path Study* - Recommendations from the cited study that relate to improving cyber career paths in the Navy.	Secretary of the Navy	90 days following enactment

Section	Matters to be Studied and Reported	Reporting Entity	Due Date for Report to Congress
		GAO	180 days after Navy report submitted
House Section 558	*Establishment of consortium of institutions of military education for cybersecurity matters* - Organization, activities, funding, actions, milestones, and research of the consortium.	Secretary of Defense	Interim report 180 days following enactment Annual reports in 2024 - 2028
SASC Section 1111	*Department of Defense Cyber and Digital Service Academy* - Evaluation of program effectiveness in recruiting and retaining scholarship recipients in the federal workforce.	Secretary of Defense	Every two years

Source: CRS analysis of legislation on Congress.gov.

Language in the SASC report (S.Rept. 117-130) accompanying the FY2023 NDAA also directs DOD to report to the Armed Services Committees on the following personnel-related topics:

- CMF manning, to include each services' manning requirements, CMF specialties, recruiting and retention challenges, education and training needs, and options to improve recruitment, retention, and career competency (by June 1, 2023);
- Information on the services' and components' use of recruitment and retention incentives (e.g., bonuses) to servicemembers in cyber career tracks over the past decade (by December 31, 2022); and
- Evaluation by the Army, Navy and Air Force of the adaptability of the Marine Corps "Cyber Auxiliary" approach to train, educate, assist, and mentor servicemembers in cyber career paths (by December 30, 2022).[43]

[43] U.S. Marine Corps, "Marine Corps Cyber Auxiliary," at https://www.hqmc.marines.mil/Agencies/Deputy-Commandant-for-Information/Information-Maneuver-Division/Marine-Corps-Cyber-Auxiliary/.

Author Information

Kristy N. Kamarck
Specialist in Military Manpower

Hibbah Kaileh
Research Assistant

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

Disclaimer