Congressional Research Service
Informing the legislative debate since 1914

FY2023 NDAA: Cyber Personnel Policies

Updated March 6, 2023

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, 117th Congress) and Senate Armed Services Committee (SASC)-reported (S. 4543, 117th Congress) Fiscal Year (FY) 2023 National Defense Authorization Act (NDAA) included 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.

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (P.L. 117-263; FY2023 NDAA), enacted on December 27, 2022, adopted many such measures. Several of the enacted provisions require DOD to strengthen organization, plans, processes, and ongoing implementation of cyber workforce initiatives and to update Congress through periodic reports and briefings. A list of selected reporting requirements, deadlines, and responsible officials is provided in the Appendix of this report.

SUMMARY

R47270

March 6, 2023

Kristy N. Kamarck
Specialist in Military Manpower

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

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]CRS In Focus IF10537, *Defense Primer: Cyberspace Operations*

The CMF's 133 teams comprise approximately 6,000 servicemembers and civilians, including reserve component personnel on active duty.[5] Reportedly, DOD expected 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 projected to add about 600 people, a 10% increase, to

[1] P.L. 114-328 §923; 10 U.S.C. §167b; U.S. Cyber Command, Our History, at https://www.cybercom.mil/About/History/. In the November 2022 DOD Dictionary of Military and Associated Terms, cyberspace is defined as "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, 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, policymakers, 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

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 CYBERCOM'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 DOD 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, and these provisions provide DOD with flexible tools to attract and retain civilians with cyber skills.[12] Prior to this law's enactment 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, as of September 2022 there were 15,000 department employees in the CES, and the Department planned 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*, 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 §1107; 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] Comment by Mark Gorak, Principal Director for Resources and Analysis in the DoD CIO's office, reported in Justin Doubleday, *White House developing cyber workforce strategy to be more 'action oriented,'* September 9, 2022, at https://federalnewsnetwork.com/cybersecurity/2022/09/white-house-developing-cyber-workforce-strategy-to-be-more-action-oriented/.

passed-version (H.R. 7900, 117th Congress) and Senate Armed Services Committee (SASC)-reported version (S. 4543, 117th Congress) of the National Defense Authorization Act for Fiscal Year 2023 (FY2023 NDAA) included several provisions that relate to recruiting, retention, and career management of DOD military and civilian personnel in cyber career fields (see **Table 1**).

Provisions enacted 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, 117th Congress)	SASC-Reported (S. 4543, 117th Congress)	Enacted (P.L. 117-263)
Reserve component (RC) and civilian staffing in response to cyber threats		
No similar provision	Section 512 would have authorized 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.	Not adopted.
No similar provision	Section 1112 would have established a civilian cybersecurity reserve pilot project to provide manpower to U.S. Cyber Command.	Section 1540 adopts the Senate provision with an amendment requiring DOD to engage with a federally funded research and development center (FFRDC) or other non-profit to assess the feasibility and advisability of creating a civilian cybersecurity reserve corps, including consideration of the results of a prior congressionally-mandated report on non-traditional cyber support.
Section 1533 would have required DOD to conduct a comprehensive review of Cyber Excepted Service policies, including personnel compensation and advancement.	Section 1114 would have required DOD to report annually on CES positions through 2028.	Section 1541 adopts elements of both House and Senate provisions.
Reviews of cyber personnel policies, strategy and planning		
Section 1531 would have required 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.	No similar provision.	Section 1502 adopts the House provision with an amendment that modifies the reporting requirements.
No similar provision.	Section 1606 would have required a DOD study on the responsibilities of the military services for organizing, training, and presenting the total force to CYBERCOM.	Section 1533 adopts the Senate provision with an amendment to modify the scope of the required report.

House-passed (H.R. 7900, 117th Congress)	SASC-Reported (S. 4543, 117th Congress)	Enacted (P.L. 117-263)
Section 1503 would have directed 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 have required the Secretary of the Navy to report on recommendations for improving cyber career paths in the Navy.	Section 1532 adopts House provision 1503 with an amendment that modifies the timeline requirements for the career designators. Section 1536 adopts Senate provision 1625.
No similar provision.	Section 1603 would have required 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 1534 adopts the Senate provision with an amendment to modify the scope of the effort.
No similar provision.	Section 1610 would have required a review of certain cyber operations personnel policies, including recruitment, retention, professional military education, personnel data sharing, structures, and departmental guidance and processes.	Not adopted.
Education and Training		
Section 558 would have required 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.	Several provisions (Sections 557, 558, and 559) in the House bill would have established various professional military education (PME) consortiums and a commission. In lieu of this, Section 557 adopts a requirement for DOD to report on the effectiveness of officer PME by December 1, 2025, with an appraisal of the feasibility and advisability of establishing a consortium.
Section 5867 would have required a financial support program at institutes of higher education designated as a Center of Academic Excellence in Cyber Education for the pursuit of programs in disciplines related to cyber or digital technology.	Section 1111 included a similar provision to House Section 5867.	Section 1535 adopts the Senate provision and directs the Secretary of Defense to establish a program that provides financial support for the pursuit of programs that are critically needed and related to cyber or digital technology.
Section 1535 would have established 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.	Not adopted.

Source: CRS analysis of legislation on Congress.gov.

Notes: Several provisions in the House-passed, SASC-reported, and enacted legislation 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.

Reserve Component and Civilian Staffing in Response to Cyber Threats

Some experts have called for leveraging the Reserve Component (RC) to meet increased federal government demand for cyber personnel. A 2017 RAND study found that over ten thousand reservists either have cyber expertise or are able to acquire cyber-related skills through civilian-based training; and many of these individuals express a desire to use these skills in the military.[15] In a March 2021 Senate Armed Services Committee Hearing, CYBERCOM Commander General 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 have expanded authorities for activating RC members and hiring civilians to respond to "significant cyber incidents."[17] Section 512 of the SASC-reported bill would have amended 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 were no similar provisions in the House-passed bill and this provision was not enacted.

Section 1112 of the SASC-reported bill would have required 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 have allowed the Army to establish criteria for selection and accession 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] The enacted FY2023 NDAA does not provide authority for an Army pilot program. Instead, it requires (under Section 1540) that DOD engage with a federally funded research and development center (FFRDC) or other independent

[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.

[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.

non-profit entity to evaluate the feasibility and advisability of such a reserve corps across DOD. This provision requires the research entity to take into consideration a study on "nontraditional cyber support" required by the FY2021 NDAA.[21] This report was to include an evaluation of different reserve models to support DOD cyber operations. Section 1540 also limits the amount of FY2023 appropriated funds that the Under Secretary of Defense for Policy may obligate or expend to not more than 75% until a copy of the FY2021 congressionally-mandated report is submitted to the Armed Services committees. This report was due to the committees in September 2022.

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 give DOD more flexibility when hiring for cyber and IT jobs.[22] Section 1541 of the FY2023 NDAA adopts elements of both House-passed and SASC-reported provisions requiring DOD to conduct a comprehensive review of the CES. Under this provision, the DOD CIO is required to report to the congressional defense committees within 30 days of completing the review with annual updates through September 30, 2028.

Reviews of cyber personnel policies, strategy, and planning

The FY2023 NDAA requires 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). These reporting requirements add to a substantial body of oversight products related to cyber personnel that Congress has required in recent years. Requirements include the "zero-based review" (ZBR) [23] of the "cyber and information technology personnel" required by section 1652 of the FY2020 NDAA (P.L. 116-92) and reports and briefings regarding cyber personnel education matters required by section 1506 of the FY2022 NDAA (P.L. 117-81), among other requirements.

Annual Budget-Cycle Reporting

Section 1502 of the FY2023 NDAA adopts a House-passed provision requiring the CYBERCOM Commander to submit a report in conjunction with the President's annual budget request to Congress[24] that evaluates the support by military departments for cyberspace operations, and CMF capability, readiness, and resourcing. This reporting requirement is first required in the FY2024 budget cycle. The FY2021 NDAA delegated responsibility to the CYBERCOM commander for directly controlling and managing the planning, programming, budgeting, and execution (PPBE) of resources starting in the FY2024 budget cycle.[25]

[21] As required by P.L. 116-283 §1730.

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

[23] A *zero-based review* is defined in this context as a "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, p. 5 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.

[24] 31 U.S.C. §1105.

[25] See 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.

Establishing a New Force Generation Model for CYBERCOM

Section 1533 of the FY2023 NDAA adopts Section 1606 of the SASC-reported bill requiring DOD to study the prospect of a new force generation model for CYBERCOM.[26] The scope of this study includes consideration of use of the RC and nonmilitary personnel[27] to support CMF teams. DOD's Principal Cyber Advisor and the CYBERCOM Commander are responsible for providing a proposed force generation plan to the Secretary of Defense no later than June 1, 2024, and the Secretary is required to submit an implementation plan to Congress no later than June 1, 2025. Section 1533 explicitly directs the Secretary of Defense to consider whether 1) the Navy should no longer be responsible for developing and providing personnel and resources to CYBERCOM, 2) whether a single military service should be responsible for providing forces to CYBERCOM, or 3) whether DOD should "create a separate service to perform the functions and missions currently performed by Cyber Mission Force units generated by multiple military services."

Navy Cyber Career Paths

In recent years, some observers have 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] Some in Navy leadership have expressed views of cyber operations as a joint endeavor, relying on other services' warfighting capabilities with support from the Navy's cryptologic warfare officers, whose mission differs from that of other cyber operators.[30] Provisions in the House-passed and SASC-reported bill specifically addressed the Navy's cyber career paths.

The FY2020 NDAA required the Secretary of the Navy to submit a report to the congressional defense committees on issues related to improving cyber career paths.[31] Section 1536 of the FY2023 NDAA requires the Navy to report on the implementation progress for recommendations made by the FY2020 congressionally-mandated report within 90 days of enactment. Section 1536 also requires a Comptroller General assessment of Government Accountability Office's implementation with an interim briefing and final report to Congress. Section 1502 of the FY2023 NDAA (discussed in "Annual Budget-Cycle Reporting") requires DOD to report on the sufficiency of career field management for cyber-related career fields across the entire CMF as part of annual budget submissions.

---

[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, at https://www.usni.org/magazines/proceedings/2022/august/navy-needs-cyber-course-correction. 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/.

[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.

[31] P.L. 116-92 §1653. CRS does not have information on whether DOD delivered the congressionally-mandated report to the defense committees on the dates they were due.

Section 1532 of the FY2023 NDAA adopts a provision in the House-passed bill directing the Secretary of the Navy to establish and sustain a specific Cyber Warfare Operations career field for uniformed personnel, that is separate and distinct from the existing cryptologic warfare and cryptologic technician career fields. The law also requires the Navy to develop 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 personnel. The enacted law precludes the Navy from assigning servicemembers with a cryptologic technician rating or cryptologic warfare officer designator to a CMF after October 1, 2025 (the House-passed bill would have required this by June 1, 2024). Some critics argue that requiring the Navy to establish a dedicated Cyber Warfare Operations career field may encourage the Navy to place a higher priority on its cyber mission, while others contend that the status quo was adequate and career field changes are unnecessary.[32]

Plan for CMF Readiness Shortfalls

Section 1534 of the FY2023 NDAA adopts section 1603 of the SASC-reported NDAA bill requiring 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 1534 also incorporates elements of section 1610 of the SASC-reported bill with respect to a review and report on policies related to the CYBERCOM Commander's authority under 10 U.S.C. §167b to monitor promotions of certain cyber operation forces.[33] Section 1534 and other provisions enacted with the FY2023 NDAA require studies, planning, and reports on matters related to recruitment, promotion, retention, and training.

Education and Training of DOD's Cyber Workforce

Certain provisions in the FY2023 NDAA 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.

Review of Professional Military Education

Section 558 of the House-passed bill would have required the Secretary of Defense to establish a consortium of military and civilian education institutions to provide a forum to share information on matters related to cybersecurity.[34] Congress previously mandated "one or more consortia of Universities to Advise Secretary of Defense on Cybersecurity Matters" in section 1659 of the FY2020 NDAA.[35] The Secretary launched a consortium, called the *University Consortium for Cybersecurity* (UC2), on December 7, 2021; it is led by the National Defense University College of Information and Cyberspace.[36] Other provisions in the House-passed version of the FY2023

[32] 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/.

[33] 10 U.S.C. §167b.

[34] 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.

[35] P.L. 116-92.

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

NDAA (Sections 557 and 559 respectively) would have created a consortium of military education institutions and a commission on professional military education to more broadly consider improvements to military education matters. The SASC-reported bill did not include similar provisions. In lieu of establishing these three separate bodies, the enacted FY2023 NDAA (Section 557) requires DOD to report to the Armed Services committees on the effectiveness of professional military education in educating officers in the Armed Forces no later than December 1, 2025. The study's mandate includes consideration if a consortium of educational institutions is feasible and advisable, and is required to include an evaluation of curriculum to include "special topics" such as cyber security and artificial intelligence. An interim briefing is due to the committees on June 1, 2023.

Department of Defense Cyber and Digital Service Academy

Section 1535 of the FY2023 NDAA adopts similar provisions in the House-passed and SASC-reported versions of the bill that require the Secretary of Defense, in consultation with DHS and the Office of Personnel Management (OPM), to establish a program called the "Department of Defense Cyber and Digital Service Academy." This program is intended to provide educational scholarships in "critical" disciplines related to cyber or digital technology. Covered disciplines 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 is authorized to 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.[37] Students who accept scholarship funding are to incur a federal employment commitment equal to the length of the scholarship. Repayment provisions would apply for failure to complete the degree requirements or post-graduation federal employment commitment. The provision requires at least 5% of the authorized funding to be directed towards associate's degrees and 50% of the authorized funding to be directed to institutions of higher education that have been awarded federal grant funding under DOD's Cyber Scholarship Program (CySP).[38] CySP currently provides recruitment and retention scholarship support to students and DOD personnel, along with capacity-building grants to institutions.[39] Congress directs the scholarship program to begin no later than the 2024 academic year.

Hacking for National Security and Public Service Innovation Program

Section 1535 of the House-passed bill would have required 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 have directed 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.[40] The SASC-reported billdid not include a similar provision and this initiative was not enacted. The Joint Explanatory Statement to accompany the FY2023 NDAA stated,

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

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

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

[40] NSIN, Hacking for Defense, at https://www.h4d.us/.

> We recognize the success of the National Security Innovation Network (NSIN) in encouraging the entry of new innovators into the national security community and believe that such a model has applicability for challenges faced by the Department of Defense and by other Federal departments and agencies. We encourage the Secretary of Defense to use existing authorities to strengthen NSIN and create additional opportunities for collaboration and shared experience between the Department of Defense, other Federal agencies, the private sector, and academia through the expansion of existing programs, partnerships, and activities, including, but not limited to, 351 such activities as Hacking for Defense, Hacking for Homeland Security, Hacking for Diplomacy, Hacking for Space, and Hacking for Manufacturing. We believe that such efforts are an important part of the Department's efforts to invest in the future of national security innovation by inspiring a new generation to public service, supporting the diversity of the United States' national security innovation workforce, and modernizing government decision-making processes.[41]

[41] Joint Explanatory Statement to Accompany the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, p. 351, at https://rules.house.gov/sites/republicans.rules118.house.gov/files/BILLS-117HR7776EAS-RCP117-70-JES.pdf.

Appendix. Selected Reporting Requirements

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

Section of FY2023 NDAA	Matter to be Studied and Reported	Reporting Entity	Due Date for Report to Congress
Section 1540	Feasibility and advisability of a DOD civilian cybersecurity reserve.	Secretary of Defense (as contracted with an FFRDC or other independent non-profit entity)	Report required Within one year of date of enactment (Dec. 27. 2023).
	Report required by Section 1730 of the FY2021 NDAA on nontraditional cyber support.	Secretary of Defense	Appropriated funds limited until DOD delivers report.
Section 1502	Annual reports on support by military departments for cyberspace operations	CYBERCOM Commander	FY2024 budget request (and annually thereafter)
Section 1534	Plan for correcting cyber mission force readiness shortfalls	Secretary of Defense, Chairman of Joint Chiefs of Staff, and Secretaries of Military Departments	Briefing required within 180 days of enactment (June 29, 2023).
Section 1533	Study and implementation plan for total force generation for the Cyberspace Operations Forces	Secretary of Defense	Progress briefings required within 90 days of enactment (March 27, 2023) and every 180 days thereafter.
		Principal Cyber Advisor and CYBERCOM Commander	Recommendations to Secretary of Defense before June 1, 2024.
		Secretary of Defense	Implementation plan submitted to Congress by June 1, 2025.
Section 1541	Comprehensive review of Cyber Excepted Service (CES).	DOD Chief Information Officer and Under Secretary of Defense for Personnel and Readiness	Report required within 30 days after review completion. Annual updates until September 30, 2028.
Section 1532	Implementation plan for the establishment of cyber operations designator and rating for the Navy.	Secretary of the Navy	Within 90 days of enactment (March 27, 2023).

Section of FY2023 NDAA	Matter to be Studied and Reported	Reporting Entity	Due Date for Report to Congress
	CYBERCOM verification that the Navy's report satisfies requirements.	CYBERCOM	Within 60 days after Navy report submitted.
Section 1536	Report on recommendations from Navy Civilian Career Path Study with implementation plans.	Secretary of the Navy	Report required within 90 days of enactment (March 27, 2023).
	Review of the Navy's implementation of recommendations.	Government Accountability Office	Report required within 180 days of Navy's report submission.
Section 557	Report on the effectiveness of Professional Military Education (PME).	Secretary of Defense with the Chairman of the Joint Chiefs of Staff and Secretaries of military departments	Interim report on June 1, 2023. Final report on December 1, 2025.
Section 1535	Information about recruitment, hiring, and retention for scholarship recipients of the Department of Defense Cyber and Digital Service Academy.	Secretary of Defense in consultation with the Office of Personnel Management	Report at a minimum of every two years following implementation (start date is 2024 academic year).

Source: CRS analysis of legislation on Congress.gov.

Author Information

Kristy N. Kamarck
Specialist in Military Manpower

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

Acknowledgments

Hibbah Kaileh contributed to research for this report.

Disclaimer