AMENDMENT TO RULES COMMITTEE PRINT 119–33

OFFERED BY MR. OGLES OF TENNESSEE

At the end of title XV of division A, add the following new subtitle:

Subtitle D—United States Cyber Force

SEC. 1551. SHORT TITLE.

This subtitle may be cited as the "United States Cyber Force Act of 2026".

SEC. 1552. FINDINGS AND PURPOSE.

(a) Findings.— Congress finds the following:

(1) Cyberspace is a distinct operational domain in which the United States faces persistent, sophisticated threats from nation-state adversaries, criminal organizations, and malicious non-state actors.

(2) The United States lacks a dedicated uniformed service charged with the protection of domestic and national-interest critical infrastructure in cyberspace, analogous to the role the Coast Guard plays in the maritime domain.

(3) Existing military cyber capabilities, including United States Cyber Command and the Cyber Mission Force, are appropriately focused on offensive and warfighting missions; they are not structured or resourced for sustained civilian-sector engagement, domestic defense, and peacetime regulatory and law-enforcement functions in cyberspace.

(4) The Cybersecurity and Infrastructure Security Agency (CISA) provides critical coordination and technical assistance but is a civilian agency without a uniformed component authorized to execute law enforcement, military support, or defense of civilian systems under title 10, United States Code.

(5) The Coast Guard model—a uniformed armed service housed in a civilian department during peacetime but capable of integration with the Navy during conflict—has proven effective in bridging domestic and military needs across the maritime domain and offers an appropriate analogue for cyberspace.

(6) A United States Cyber Force would fill this structural gap, providing a uniformed service that maintains cyber domain awareness, defends domestic and allied critical infrastructure, develops and enforces cyber domain law and norms, and is capable of full integration into the joint force during hostilities.

(7) The establishment of a Reserve and Auxiliary to the Cyber Force would offer opportunities for deeper relationships between the public and private sector in the cyber domain.

(b) Purpose.— The purpose of this subtitle is to establish the United States Cyber Force as an armed service of the United States, organized within the Department of Homeland Security during peacetime, with the authority and capability to operate as a service of the Department of the Air Force during time of war or when the President so directs.

SEC. 1553. DEFINITIONS.

In this subtitle:

(1) Commandant.— The term "Commandant" means the Commandant of the Cyber Force.

(2) Cyber Force.— The term "Cyber Force" means the United States Cyber Force established under section 1554.

(3) Cyberspace.— The term "cyberspace" has the meaning given that term in Presidential Policy Directive 20, and includes all networked information systems, communications infrastructure, industrial control systems, and digital environments owned or operated by Federal, State, local, Tribal, and territorial governments, critical infrastructure sectors, and United States persons.

(4) Critical Infrastructure.— The term "critical infrastructure" has the meaning given that term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)).

(5) Department.— The term "Department" means the Department of Homeland Security.

(6) Secretary.— The term "Secretary" means the Secretary of Homeland Security, except where context requires reference to the Secretary of Defense or the Secretary of the Air Force.

SEC. 1554. ESTABLISHMENT OF THE UNITED STATES CYBER FORCE.

(a) Establishment.— There is established within the Department of Homeland Security an armed service to be known as the United States Cyber Force.

(b) Status as Armed Service.— The Cyber Force is an armed service of the United States within the meaning of title 10, United States Code, and a uniformed service of the United States within the meaning of title 37, United States Code.

(c) Status as Military Service.— The Cyber Force shall be organized, trained, and equipped to provide military forces necessary for—

(1) the defense of cyberspace as a domain;

(2) the protection of United States critical infrastructure in cyberspace;

(3) the enforcement of Federal laws governing cyberspace, to the extent authorized; and

(4) the execution of cyber operations in support of national defense.

(d) Dual Character.— The Cyber Force shall at all times be a branch of the Armed Forces of the United States operating as a service in the Department of Homeland Security, except when operating as a service in the Department of the Air Force as provided in section 1558.

SEC. 1555. ORGANIZATION.

(a) Headquarters.— The headquarters of the Cyber Force shall be located in the National Capital Region, co-located with or in proximity to the headquarters of the Cybersecurity and Infrastructure Security Agency.

(b) Components.— The Cyber Force shall consist of—

(1) the Regular Cyber Force;

(2) the Cyber Force Reserve;

(3) the Cyber Force Auxiliary; and

(4) such other components as the Commandant may establish.

(c) Districts and Sectors.— The Cyber Force shall be organized into cyber districts and sectors, aligned—where appropriate—with the CISA regional structure, the Defense Industrial Base sector, and the critical infrastructure sector definitions established under Presidential Policy Directive 21.

(d) Integration With CISA.— The Cyber Force shall maintain a close operational relationship with the Cybersecurity and Infrastructure Security Agency, including co-location of joint operations centers, and shall not duplicate the civilian advisory functions of such Agency. Memoranda of agreement governing deconfliction, information sharing, and operational primacy shall be negotiated and updated on a biennial basis.

SEC. 1556. MISSION AND FUNCTIONS.

(a) Primary Mission.— The primary peacetime mission of the Cyber Force is the defense of United States cyberspace, including protection of critical infrastructure, detection and response to malicious cyber activity, and maintenance of cyber domain awareness.

(b) Core Functions.— The Cyber Force shall perform the following functions:

(1) Conduct continuous monitoring of Federal civilian executive branch networks and, upon request or pursuant to applicable law, the networks of critical infrastructure entities, to detect, characterize, and respond to cyber threats and incidents.

(2) Provide hunt, incident response, and remediation capabilities to Federal, State, local, Tribal, and territorial governments and, where authorized, to private critical infrastructure operators.

(3) Develop and enforce cyber domain standards, rules of engagement, and regulatory frameworks, analogous to the role of the Coast Guard in administering maritime law and safety regulations.

(4) Conduct cyber domain law enforcement activities as authorized by Federal statute, including investigation of cyber crimes in coordination with the Federal Bureau of Investigation and the United States Secret Service.

(5) Maintain a Cyber Domain Recognized Picture—a persistent, classified, and unclassified view of threat actor activity, vulnerability landscapes, and infrastructure status—and disseminate that picture to relevant Federal and private-sector stakeholders.

(6) Provide defense support to civil authorities following cyber incidents, including major cyber attacks on electoral infrastructure, financial systems, health systems, and utilities.

(7) Develop doctrine, tactics, techniques, and procedures for cyber domain operations that can be shared with allied and partner nations.

(8) Support the National Cyber Director and the Director of National Intelligence in producing assessments of foreign cyber threats and capabilities.

(c) Limitation.— Nothing in this section authorizes the Cyber Force to conduct offensive cyber operations against targets within the United States or to conduct surveillance of United States persons inconsistent with the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or the Fourth Amendment to the Constitution of the United States.

SEC. 1557. RELATIONSHIP TO THE DEPARTMENT OF HOMELAND SECURITY.

(a) Administrative Authority.— Except as provided in section 1558, the Cyber Force shall be administered by the Secretary of Homeland Security. The Secretary shall—

(1) prescribe regulations for the governance of the Cyber Force;

(2) exercise administrative authority over personnel, procurement, and operations of the Cyber Force;

(3) submit budget requests for the Cyber Force as part of the budget of the Department of Homeland Security; and

(4) report to Congress on the activities, personnel, and readiness of the Cyber Force.

(b) Independence of Military Functions.— Notwithstanding subsection (a), the Commandant of the Cyber Force retains authority over the military organization, training, equipping, and readiness of the Cyber Force and may communicate directly with the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Commander of United States Cyber Command on matters of military readiness and joint operations.

(c) Joint Requirements.— The Commandant shall be a member of the Joint Chiefs of Staff, with the same status and authorities as the Commandant of the Coast Guard under section 151 of title 10, United States Code.

(d) National Security Council Participation.— The Commandant shall participate in interagency cyber policy processes, including those coordinated by the National Security Council and the Office of the National Cyber Director, in the same manner as the Commandant of the Coast Guard participates in relevant interagency processes.

(e) Liaison and Coordination With Service Cyber Components.—

(1) LIAISON FRAMEWORK.—The Commandant shall establish reciprocal liaison officer arrangements with United States Cyber Command and with the cyber component commands of the Army, Navy, Air Force, Marine Corps, and Space Force, for the purpose of coordinating defensive cyber operations, sharing threat intelligence, and deconflicting activities on networks of shared interest.

(2) JOINT EXERCISES.—The Cyber Force shall participate in not fewer than one joint cyber exercise each fiscal year with one or more service cyber component

commands, and the Commandant shall report annually to the congressional defense committees on the results of such participation.

(3) TECHNICAL STANDARDS.—The Commandant shall participate in Department of Defense cybersecurity standards processes, including security technical implementation guides and the risk management framework, to ensure interoperability of Cyber Force tools and platforms with the joint force.

SEC. 1558. SERVICE UNDER THE DEPARTMENT OF THE AIR FORCE.

(a) Transfer Authority.— Upon the declaration of war, the declaration of a national emergency, or when the President so directs by Executive order, the Cyber Force, or such elements thereof as the President directs, shall operate as a service in the Department of the Air Force under the authority of the Secretary of the Air Force, in the same manner that the Coast Guard operates as a service in the Department of the Navy under section 3 of title 14, United States Code.

(b) Operational Control.— Upon transfer under subsection (a)—

(1) the Commandant shall report to the Secretary of the Air Force;

(2) the Cyber Force shall be subject to the Uniform Code of Military Justice and applicable provisions of title 10, United States Code, to the same extent as other armed services operating under the Department of the Air Force;

(3) the Cyber Force may be assigned to the operational control of the Commander of United States Cyber Command or another combatant commander as the President directs; and

(4) the Secretary of Homeland Security shall retain administrative responsibilities relating to civilian personnel and non-military functions of the Cyber Force not transferred under this section.

(c) Relationship to Space Force.— The Secretary of Defense, acting through the Secretary of the Air Force, may establish a formal integration framework between the Cyber Force and the Space Force for the purpose of—

(1) coordinating defense of space-enabled cyber infrastructure, including satellite communications and systems dependent on the Global Positioning System;

(2) conducting joint operations in the space-cyber nexus;

(3) sharing personnel, training pipelines, and technical platforms where appropriate; and

(4) presenting a unified cyber and space domain awareness picture to national command authorities.

(d) Reversion.— Upon the termination of the conditions giving rise to a transfer under subsection (a), the President shall, by Executive order, return the Cyber Force to operation as a service in the Department of Homeland Security. A period of not less than 180 days shall be provided for orderly reversion of administrative functions.

SEC. 1559. COMMANDANT OF THE CYBER FORCE.

(a) Appointment.— The Cyber Force shall be led by a Commandant of the Cyber Force, who shall be appointed by the President, by and with the advice and consent of the Senate, from among officers of the Cyber Force serving in the grade of vice admiral or above (or the equivalent). The Commandant shall serve a term of four years and shall be compensated at the rate applicable to the Commandant of the Coast Guard.

(b) Responsibilities.— The Commandant shall—

(1) be responsible to the Secretary of Homeland Security for the administration and operation of the Cyber Force;

(2) prescribe regulations for the discipline, training, and readiness of the Cyber Force;

(3) serve as the principal military advisor on cyber domain operations to the Secretary of Homeland Security, the Secretary of Defense, and the President; and

(4) represent the Cyber Force on the Joint Chiefs of Staff pursuant to section 1557(c).

(c) Vice Commandant.— There shall be a Vice Commandant of the Cyber Force, appointed in the same manner as the Commandant, who shall perform such duties as the Commandant may direct and act as Commandant during the absence or disability of the Commandant.

SEC. 1560. PERSONNEL AUTHORITIES.

(a) Officer Corps.— The Cyber Force shall have a commissioned officer corps organized into grades corresponding to those established for the Coast Guard under chapter 21 of title 14, United States Code. The President may establish additional grades as appropriate for a cyber-specialized service.

(b) Enlisted Personnel.— The Cyber Force shall have an enlisted force with grades, training pipelines, and career tracks developed to reflect the technical requirements of cyber domain operations.

(c) Pay and Benefits.— Members of the Cyber Force shall receive the same pay, allowances, and benefits as members of the Coast Guard of equivalent grade and time in service, pursuant to title 37, United States Code.

(d) Cyber-Specific Incentive Pay.— The Commandant, with the approval of the Secretary, may establish cyber-specific retention, recruitment, and special duty assignment pay for members with critical cyber skills, in the same manner and subject to the same limitations as special pay authorities available to other armed services.

(e) Civilian Workforce.— The Cyber Force shall employ a civilian workforce under the authorities applicable to the Department of Homeland Security and, during a transfer under section 1558, the Department of the Air Force. The Commandant shall ensure that civilian technical expertise is retained across transfers between departments.

(f) Commissioning Sources.— The Commandant may establish a Cyber Force Academy or, in lieu thereof, develop a curriculum and commissioning pipeline in cooperation with the United States Military Academy, the United States Naval Academy, the United States Air Force Academy, the United States Coast Guard Academy, and civilian institutions for the

purpose of producing officers with the technical and military competencies required by the Cyber Force.

SEC. 1561. CYBER FORCE RESERVE AND AUXILIARY.

(a) Cyber Force Reserve.— There is established a Cyber Force Reserve, which shall be organized and administered in the same manner as the Coast Guard Reserve under chapter 37 of title 14, United States Code, and shall be subject to involuntary activation in the same circumstances and under the same conditions.

(b) Cyber Force Auxiliary.— There is established a Cyber Force Auxiliary consisting of voluntary civilian cyber professionals who agree to support Cyber Force missions under the supervision of the Commandant. The Auxiliary shall—

(1) provide surge capacity for incident response operations;

(2) support community cyber resilience and public outreach; and

(3) be organized, equipped, and authorized analogously to the Coast Guard Auxiliary under chapter 39 of title 14, United States Code.

(c) Coordination With Civilian Cybersecurity Reserve Corps Pilot Program.— In establishing the Cyber Force Reserve and Auxiliary, the Commandant shall coordinate with the Secretary of Defense regarding the pilot program required by section 1506 of this Act, and shall incorporate the lessons of such pilot program into the design of the Auxiliary.

(d) Industry Talent Exchange.— The Commandant shall establish a formal talent exchange program with private-sector critical infrastructure operators to facilitate movement of personnel between the Cyber Force and relevant private entities.

SEC. 1562. AUTHORITIES AND POWERS.

(a) Law Enforcement Authority.— Members of the Cyber Force designated by the Commandant, with the concurrence of the Secretary, shall have the authority to—

(1) execute warrants and make arrests for offenses against the United States in cyberspace, in cooperation with the Department of Justice;

(2) seize, pursuant to process, property involved in violation of Federal law governing cyberspace; and

(3) perform other law enforcement duties consistent with applicable statutes and civil liberties protections.

(b) Cyber Domain Regulatory Authority.— The Commandant may prescribe, with the approval of the Secretary, regulations governing cybersecurity standards for vessels in waters of the United States (in coordination with the Coast Guard), operators of critical infrastructure required to interface with Federal networks, and Federal contractors subject to the Federal Acquisition Regulation, to the extent not otherwise preempted.

(c) International Engagement.— The Commandant may enter into agreements with foreign military and law enforcement counterparts for cyber domain cooperation, subject to the approval of the Secretary of State and in coordination with the Secretary of Defense and the Director of National Intelligence.

(d) Limitation on Domestic Surveillance.— Nothing in this section or any other provision of this subtitle authorizes the Cyber Force to collect, store, or process the communications of United States persons except as authorized by the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) or chapter 119 of title 18, United States Code.

SEC. 1563. CONFORMING AMENDMENTS.

(a) Title 10.— Section 101(a)(4) of title 10, United States Code, is amended by inserting "the Cyber Force," after "the Space Force,".

(b) Title 14.— Chapter 1 of title 14, United States Code, is amended by adding at the end the following new section:

"§ 103. Relationship to the Cyber Force

"The Coast Guard may, at the direction of the President, coordinate operations with the Cyber Force in the maritime cyber domain, including defense of vessel systems, port facility control systems, and maritime navigation infrastructure against cyber attack.".

(c) Joint Chiefs of Staff.— Section 151(a) of title 10, United States Code, is amended by adding at the end the following new paragraph:

"(8) The Commandant of the Cyber Force.".

(d) Further Amendments.— The Secretary of Defense and the Secretary of Homeland Security shall jointly submit to Congress, not later than 180 days after the date of the enactment of this Act, a comprehensive list of additional conforming amendments required to give full effect to this subtitle, together with proposed legislative language.

SEC. 1564. TRANSITION PLANNING AUTHORIZATION; FUNDING PLAN.

(a) Transition Planning Authorization.— There is authorized to be appropriated to the Department of Homeland Security $25,000,000 for fiscal year 2027 for the purpose of developing the transition plan required under section 1565, including costs of personnel, interagency coordination, contracting for technical assistance, and associated administrative expenses. No funds authorized under this subsection shall be used for the operational establishment of Cyber Force units, the procurement of major systems, or the construction or leasing of facilities beyond those necessary to house the transition planning office.

(b) Funding Plan.— The Secretary of Defense and the Secretary of Homeland Security shall, not later than 180 days after submission of the transition plan under section 1565(a), jointly submit to the Committee on Armed Services and the Committee on Homeland Security of the House of Representatives, and the Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate, a comprehensive funding plan for the establishment and operation of the Cyber Force for fiscal years 2028 through 2033. The funding plan shall include—

(1) specific dollar amounts requested for each fiscal year, organized by appropriations account and by major program element;

(2) a cost estimate prepared by the Director of Cost Assessment and Program Evaluation, consistent with the requirements of section 2334 of title 10, United States Code;

(3) identification of any functions or personnel proposed to be transferred from existing Federal entities, together with the associated funding offsets; and

(4) a certification by the Director of the Office of Management and Budget that the funding plan is consistent with the most recent baseline projections under the Congressional Budget Act of 1974.

(c) Subsequent Authorization Required.— Operational funding for the Cyber Force for fiscal year 2028 and each subsequent fiscal year shall be authorized in the national defense authorization Act for that fiscal year or in a separate authorization Act. No funds shall be appropriated for the operational establishment or sustainment of the Cyber Force until such authorization is enacted. The Secretaries shall update the funding plan required under subsection (b) annually, concurrent with submission of the budget of the President.

(d) Limitation on Duplication.— No funds authorized under subsection (a) or subsequently appropriated for the Cyber Force pursuant to subsection (c) shall be used to duplicate or supplant the existing civilian workforce or cybersecurity advisory functions of the Cybersecurity and Infrastructure Security Agency. The Secretary shall certify annually to the committees of jurisdiction that appropriations for the Cyber Force do not result in displacement of the civilian capabilities of such Agency.

SEC. 1565. TRANSITION PROVISIONS.

(a) Transition Plan.— The Secretary of Homeland Security, in consultation with the Secretary of Defense and the Director of the Cybersecurity and Infrastructure Security Agency, shall develop and implement a transition plan for the establishment of the Cyber Force not later than 2 years after the date of the enactment of this Act. The transition plan shall include—

(1) a description of personnel and functions to be transferred to the Cyber Force from existing Federal entities;

(2) a plan for the development of a commissioned officer corps, including commissioning sources and training pipelines;

(3) a plan for the establishment of the Cyber Force Reserve and Auxiliary;

(4) deconfliction protocols with the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the National Security Agency, and United States Cyber Command;

(5) the results of the review conducted under section 1503 of this Act, as relevant to the realignment of Department of Defense cybersecurity responsibilities affected by the establishment of the Cyber Force; and

(6) a proposed statutory framework governing the transfer of the Cyber Force to the Department of the Air Force.

(b) Voluntary Transfer.— Members of the Cyber National Mission Force, defensive cyber operations forces, the cybersecurity division of the Cybersecurity and Infrastructure

Security Agency, and other relevant Federal military and civilian employees may voluntarily transfer to the Cyber Force under terms established by the Commandant and the applicable head of department or agency, subject to applicable civil service and collective bargaining requirements.

(c) Interim Leadership.— Until a Commandant is appointed and confirmed, the Secretary shall designate a senior official to perform the functions of the Commandant for purposes of implementing this subtitle.

(d) Report to Congress.— Not later than 1 year after the date of the enactment of this Act, and annually thereafter for 5 years, the Secretary shall transmit to the Committee on Armed Services and the Committee on Homeland Security of the House of Representatives, and the Committee on Armed Services and the Committee on Homeland Security and Governmental Affairs of the Senate, a report on implementation of this subtitle, including the status of the transition plan, personnel levels, and operational readiness.

SEC. 1566. EFFECTIVE DATE.

This subtitle shall take effect on the date that is 180 days after the date of the enactment of this Act, or such earlier date as the President may establish by Executive order.