THIS WEBSITE IS AN ACADEMIC EXERCISE AND PUBLIC POLICY PROPOSAL. IT IS A DRAFT OF A PRESIDENTIAL ACTION WHICH COULD BE TAKEN TO CREATE A U.S. CYBER FORCE AND CYBER NATIONAL GUARD. THIS DOCUMENT IS NOT AN OFFICIAL PRESIDENTIAL DIRECTIVE, NOR DOES IT REPRESENT ANY OFFICIAL POLICIES OR POSITIONS OF THE WHITE HOUSE, THE DEPARTMENT OF WAR, THE DEPARTMENT OF THE ARMY, THE U.S. ARMY, THE NATIONAL GUARD BUREAU, OR THE VIRGINIA NATIONAL GUARD.

Cyber Policy Directive–1

Academic public policy proposal · November 19, 2026

I propose that the President direct the Secretary of War to prepare legislation establishing a United States Cyber Force within the Department of the Army, with the Cyber National Guard as its sole reserve component. The new service would organize, train, and equip military cyberspace forces. U.S. Cyber Command would retain operational command.

MEMORANDUM FOR

- THE VICE PRESIDENT
- THE SECRETARY OF STATE
- THE SECRETARY OF WAR
- THE ATTORNEY GENERAL
- THE SECRETARY OF COMMERCE
- THE SECRETARY OF ENERGY
- THE SECRETARY OF HOMELAND SECURITY
- THE SECRETARY OF THE ARMY
- THE SECRETARY OF THE NAVY
- THE SECRETARY OF THE AIR FORCE
- THE WHITE HOUSE CHIEF OF STAFF
- THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND BUDGET
- THE DIRECTOR OF NATIONAL INTELLIGENCE
- THE ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
- THE ASSISTANT TO THE PRESIDENT AND DEPUTY CHIEF OF STAFF FOR POLICY
- THE HOMELAND SECURITY ADVISOR
- THE ASSISTANT TO THE PRESIDENT FOR SCIENCE AND TECHNOLOGY
- THE ASSISTANT TO THE PRESIDENT AND DIRECTOR OF LEGISLATIVE AFFAIRS
- THE NATIONAL CYBER DIRECTOR
- THE CHAIRMAN OF THE JOINT CHIEFS OF STAFF
- THE CHIEF OF THE NATIONAL GUARD BUREAU
- THE COMMANDER, UNITED STATES CYBER COMMAND
- THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
- THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
- THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SUBJECT: Establishment of the United States Cyber Force and Cyber National Guard

Section 1. Introduction and Policy.

Cyberspace is integral to the American way of life, national security, economic prosperity, and modern warfare. Our adversaries increasingly threaten American critical infrastructure and contest our military superiority in cyberspace. The organization of military cyberspace forces among the existing armed services presents challenges to unified force development and readiness. It is imperative that the United States adapt its military institutions to deter aggression, defend the Nation, and maintain superiority in cyberspace.

Toward that end, the Department of War shall take actions under existing authority to strengthen American military cyberpower and develop a legislative proposal to establish the United States Cyber Force as a distinct armed service within the Department of the Army, with the Cyber National Guard as its sole reserve component. The proposed Cyber Force would organize, train, and equip military cyberspace forces for joint operations, while United States Cyber Command would retain operational command. The Cyber National Guard would strengthen national defense and state cyber resilience consistent with applicable law.

Section 2. Definitions.

For purposes of this memorandum and the legislative proposal directed by section 3:

(a) "United States Cyber Force" refers to a proposed armed service within the Department of the Army responsible for organizing, training, and equipping military cyberspace forces.

(b) "Cyber National Guard" refers to a proposed third component of the National Guard, consisting of state-organized, federally recognized forces, with a corresponding federal reserve component serving as the sole reserve component of the United States Cyber Force.

(c) "United States Cyber Command" refers to the existing Unified Combatant Command responsible for military cyberspace operations under 10 U.S.C. § 167b and the Unified Command Plan.

Section 3. Legislative Proposal and Decision.

(a) Within 120 days of the date of this memorandum, the Secretary of War shall submit to the President, through the Office of Management and Budget, a legislative proposal to establish the United States Cyber Force as a new armed service within the Department of the Army, with the Cyber National Guard as its sole reserve component.

(b) The proposed United States Cyber Force and Cyber National Guard shall be designed to:

(i) Defend the American people, the United States homeland, and national interests against aggression in cyberspace, while supporting allies and partners consistent with U.S. defense priorities;

(ii) Establish and maintain American military superiority in cyberspace;

(iii) Provide decisive offensive and defensive capabilities to joint and coalition forces;

(iv) Develop and sustain a professional military cyber workforce;

(v) Strengthen national defense and state cyber resilience; and

(vi) Advance Super Intelligence-enabled military capabilities consistent with applicable law.

(c) The Secretary shall consult the military departments, United States Cyber Command, the National Guard Bureau, and affected federal and state authorities. The legislative proposal shall compare the proposed Cyber Force with continued implementation of CYBERCOM 2.0 and other reforms under existing authorities, assessing effects on warfighting readiness, force generation, personnel, costs, and service-retained capabilities. The proposal shall identify necessary statutory amendments and resource transfers, preserve effective existing initiatives, and minimize duplicative organizations and functions.

(d) Subject to presidential approval and applicable Office of Management and Budget clearance, the White House Office of Legislative Affairs shall seek congressional authorization through the Fiscal Year 2029 National Defense Authorization Act or an earlier appropriate legislative vehicle.

Section 4. Scope.

(a) The legislative proposal required by section 3 of this memorandum shall include provisions that would, if enacted:

(i) consolidate existing military cyberspace forces and functions, as appropriate, to eliminate duplication and strengthen joint readiness;

(ii) preserve the statutory responsibilities of United States Cyber Command under 10 U.S.C. § 167b and the mission-essential cyberspace capabilities of the existing armed services; and

(iii) not include the National Security Agency, other elements of the Intelligence Community, the Cybersecurity and Infrastructure Security Agency, or other civilian cybersecurity organizations.

(b) The Secretary of War shall identify proposed transfers of personnel, missions, programs, and resources, preserving operational continuity, service-specific capabilities, and existing National Security Systems authorities.

Section 5. Super Intelligence-Enabled Cyberspace Capabilities.

The legislative proposal required by section 3 of this memorandum shall designate the United States Cyber Force as the principal military service for developing, integrating, testing, fielding, and sustaining Super Intelligence-enabled capabilities for assigned military cyberspace missions. The Secretary of War shall account for existing United States Cyber Command acquisition and modernization programs and other Department-wide advanced technology initiatives, avoid duplication, and ensure consistency with National Security Presidential Memoranda 11 and 12. Such capabilities shall strengthen joint military operations while preserving existing statutory authorities, appropriate human oversight, system reliability, and military command accountability.

Section 6. Cyber National Guard.

(a) The legislative proposal required by section 3 of this memorandum shall establish the Cyber National Guard as a third component of the National Guard, alongside the Army National Guard and Air National Guard, with a corresponding federal reserve component serving as the sole reserve component of the United States Cyber Force. The Cyber National Guard shall be state-organized, federally recognized, and available for lawful federal and state missions.

(b) The proposed Cyber National Guard should build upon existing military cyber capabilities to organize, train, and equip forces for national defense and civilian-led domestic cyber response, including regional incident response and interstate assistance.

(c) The Chief of the National Guard Bureau, in consultation with the Secretary of the Army, governors, and adjutants general, shall coordinate plans for the Cyber National Guard's organization, funding, and readiness.

(d) The legislative proposal shall address employment under Title 10, Title 32, and state active duty, preserving gubernatorial command of non-federalized forces and lawful federal mobilization. The Secretary of War shall develop arrangements for state cyber-defense continuity during federal mobilization, consistent with civilian incident authority and lawful access to civilian systems.

Section 7. Personnel, Accessions, and Education.

(a) The Secretary of War, in consultation with the Secretaries of the military departments, United States Cyber Command, and the Chief of the National Guard Bureau, shall develop a personnel and professional development framework for the proposed United States Cyber Force and Cyber National Guard. The legislative proposal required by section 3 of this memorandum shall establish appropriate accession, career development, and advancement authorities for military and civilian cyberspace professionals.

(b) The proposed United States Cyber Force and Cyber National Guard should:

(i) recruit, develop, and retain highly qualified cyberspace personnel through competitive compensation, specialized career tracks, and advancement based upon technical proficiency and military effectiveness;

(ii) establish appropriate enlisted, warrant officer, commissioned officer, and civilian career pathways, including direct commissioning, interservice transfers, and recognition of relevant professional experience;

(iii) develop specialized education and training programs in offensive and defensive cyberspace operations, operational technology, advanced technologies, and joint military operations; and

(iv) strengthen partnerships with military education institutions, universities, research organizations, and industry to advance technical expertise, professional development, and operational readiness.

(c) The Secretary of War shall assess existing military and National Guard training institutions and determine whether additional specialized facilities, including a Cyber National Guard Operational Technology Center of Excellence, are necessary to meet validated requirements. Such assessment shall consider cost, existing infrastructure, and opportunities to consolidate or expand current capabilities.

Section 8. Budget.

In accordance with the Department of War budget process, the Secretary of War shall submit to the Director of the Office of Management and Budget a proposed budget for the United States Cyber Force and Cyber National Guard for consideration in the President's Fiscal Year 2029 Budget Request, including five-year cost estimates distinguishing existing resources proposed for transfer from additional funding requirements.

Section 9. United States Cyber Force Organization and Leadership.

(a) The legislative proposal required by section 3 of this memorandum shall establish the United States Cyber Force within the Department of the Army, under the civilian authority of the Secretary of the Army.

(b) The legislative proposal shall establish a Chief of Cyberspace Operations in the grade of General, who shall serve as a member of the Joint Chiefs of Staff.

(c) The legislative proposal shall establish a Director of the Cyber National Guard in the grade of Lieutenant General, appointed by the President by and with the advice and consent of the Senate, who shall serve under the Chief of the National Guard Bureau.

(d) The Secretary of War shall assess proposed leadership positions, headquarters requirements, and personnel authorizations against existing military structures and directed general officer reductions,

identifying opportunities to consolidate headquarters, eliminate duplicative functions, and offset proposed senior-officer billets without impairing warfighting readiness.

Section 10. Associated Elements.

(a) United States Cyber Command shall retain its statutory and operational responsibilities under 10 U.S.C. § 167b and the Unified Command Plan, including joint training, certification, and operational employment of military cyberspace forces. The proposed United States Cyber Force shall organize, train, and equip such forces for employment by United States Cyber Command.

(b) With forces provided by the United States Cyber Force and other armed services, United States Cyber Command shall conduct authorized cyberspace operations to defend the Nation, deter aggression, maintain American military superiority, and support joint and coalition forces across the spectrum of conflict.

Section 11. Relationship with National Intelligence.

The Secretary of War and the Director of National Intelligence shall strengthen collaboration between the Department of War and the Intelligence Community to increase unity of effort and the effectiveness of military cyberspace operations, consistent with existing statutory authorities. Within 90 days of the date of this memorandum, they shall report to the President on measures taken and proposed to improve intelligence integration and operational coordination, including legislative proposals as necessary and appropriate.

Section 12. Operational Authorities.

The National Security Council, in coordination with the National Cyber Director, shall conduct an accelerated review of operational authorities for the proposed United States Cyber Force and Cyber National Guard and existing United States Cyber Command. Within 90 days of the date of this memorandum, the Secretary of War shall submit proposed authority changes to the National Security Council. Within 30 days thereafter, the Council shall complete an interagency review and recommend appropriate changes to the President, distinguishing measures available under existing law from those requiring congressional authorization.

Section 13. Periodic Review.

The Secretary of War shall report to the President every 180 days on legislative progress and, following congressional authorization, the implementation, costs, and readiness of the United States Cyber Force and Cyber National Guard. The Secretary shall conduct periodic reviews to determine whether additional organizational reforms or legislative authorities are necessary to strengthen American military superiority in cyberspace.

Section 14. General Provisions.

(a) Nothing in this memorandum shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof, including the authorities of United States Cyber Command and the several States; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This memorandum shall be implemented consistent with applicable law, national security requirements, and the availability of appropriations. Nothing herein shall establish a new armed service or National Guard component without congressional authorization or confer additional military, intelligence, law-enforcement, or civilian-system-access authorities.

(c) The designation "Secretary of War" refers to the Secretary of Defense under Executive Order 14347 and does not alter the Secretary's statutory authorities.

(d) This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity against the United States, its agencies, officers, employees, or agents, or any other person.

(e) The Secretary of War is authorized and directed to publish this memorandum in the Federal Register.

###

Disclaimer

THIS WEBSITE IS AN ACADEMIC EXERCISE AND PUBLIC POLICY PROPOSAL. IT IS A DRAFT OF A PRESIDENTIAL ACTION WHICH COULD BE TAKEN TO CREATE A U.S. CYBER FORCE AND CYBER NATIONAL GUARD.

THIS DOCUMENT IS NOT AN OFFICIAL PRESIDENTIAL DIRECTIVE, NOR DOES IT REPRESENT ANY OFFICIAL POLICIES OR POSITIONS OF THE WHITE HOUSE, THE DEPARTMENT OF WAR, THE DEPARTMENT OF THE ARMY, THE U.S. ARMY, THE NATIONAL GUARD BUREAU, OR THE VIRGINIA NATIONAL GUARD.

Mateo T. Portelli

I am a graduate student at Old Dominion University, where I am pursuing a Master of Science in Cybersecurity. My academic interests include critical infrastructure resilience and how the United States organizes its military cyber forces. I earned my Bachelor of Arts in History from the University of Nevada, Las Vegas. I also serve as a Cyber Warfare Officer in the Virginia Army National Guard.

Mateo@MartelloPieto.com · LinkedIn