Joint Action Plan for State-Federal Unity of Effort on Cybersecurity

EXECUTIVE SUMMARY

The Council of Governors (hereafter, referred to as the "Council"), consistent with Section 1822 of the National Defense Authorization Act for Fiscal Year 2008 (Public Law 110-181), was established by Executive Order (EO) 13528, *Establishment of the Council of Governors*, issued on January 11, 2010, "to strengthen further the partnership between the Federal Government and State governments to protect our Nation and its people and property."

Federal-state cooperation is critical to protecting communities given the evolving challenges and threats facing our country, which range from extreme weather to domestic and international terrorism to a global pandemic. Enhancing the Nation's cybersecurity resilience has evolved into a top priority for the Council because of the increased and evolving cybersecurity threats to the U.S. Homeland over the last decade.

Today, the bi-partisan Council continues to have growing concerns over the protection of our nation's critical infrastructure. Protection of our nation's critical infrastructure is a shared responsibility of the owners and operators of that infrastructure, the Federal Government, and state, local, tribal and territorial (SLTT) governments.

In 2014, the Council worked with Federal officials to develop a Joint Action Plan for State-Federal Unity of Effort on Cybersecurity (hereafter, referred to as the "Plan"), that describes the importance of promoting a national approach to preventing, protecting against, mitigating, responding to, and recovering from cyber incidents[1], including the development or refinement of a national cyber incident response framework.

In 2019, the Council of Governors and its Federal participants (i.e., the Federal officials identified in section 2 of EO 13528, and appropriate officials of other executive departments or agencies as may be designated by the Secretary of Defense or the Secretary of Homeland Security) (hereinafter referred to collectively as "the Parties")

[1] A "cyber incident," according to Presidential Policy Directive 41 (PPD-41, "United States Cyber Incident Coordination," is defined as "[a]n event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this directive, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

decided that the Plan should remain the enduring foundational document and be reviewed periodically to evaluate its effectiveness. Additionally, after such a review, any recommended changes must be approved by all the Parties.

Since 2020, the cybersecurity threats facing the U.S. Homeland have increased and the Nation and states, more than ever, are in a heightened posture when it comes to cybersecurity and protecting the most critical infrastructure and assets. As a result, in 2022, the Parties agreed that the Council's Cybersecurity Working Group would recommend changes to update and improve the "Plan," which is presented in this document. This document represents the first revision of the original 2014 Joint Action Plan for State-Federal Unity of Effort on Cybersecurity.

STATEMENT OF PRINCIPLES

Preamble

The Parties adopt the principles and actions for State-Federal unity of effort, described below, to strengthen the Nation's security and resilience against cybersecurity threats. The Council consists of ten state governors appointed to two-year terms by the President – no more than five of whom may be from the same political party. The president also designates two governors, who are not members of the same political party, to serve as co-chairs of the Council. Executive Order (EO) 13528, *Establishment of the Council of Governors*, further identifies the following Federal officials as those with whom the views, information, or advice of the Counsel should be exchanged: the Secretary of Defense, the Secretary of Homeland Security, the Assistant to the President for Homeland Security, the Assistant to the President for Intergovernmental Affairs, the Commander of U.S. Northern Command, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (now the Assistant Secretary of Defense for Homeland Defense and Hemispheric Affairs), the Commandant of the Coast Guard, and the Chief of the National Guard Bureau (NGB). Other key Federal officials such as the Administrator of the Federal Emergency Management Agency (FEMA), the Director of the Cybersecurity and Infrastructure Security Agency (CISA), the Secretaries of the Army and the Air Force, and the Chiefs of Staff of the Army and the Air Force have been designated as regular participants by the Secretary of Defense or the Secretary of Homeland Security.

As adopted, this document is a framework for establishing a collaborative environment for States, territories, and the Federal Government to expedite and enhance the Nation's response[i] to cyber incidents; to improve cyber threat and vulnerability information sharing; to utilize common capabilities and resources as appropriate, including the National Guard, to support State and Federal cyber missions; and to secure and/or defend U.S. access to and use of cyberspace, including securing and/or defending State and Federally owned or operated critical infrastructure and key resources from cyberspace threats, in accordance with existing State and Federal laws, regulations, and policies.

This Plan is a collaborative effort of the Parties. Following the acceptance of this Plan, the Parties will work expeditiously to implement all specified actions.

Principles

- The Nation benefits when State, territorial and Federal entities fully utilize their authorities and resources in cooperation. This Plan does not alter Federal and State law or existing legal authority. All expressed and implied powers of the President, the Governors, and the heads of Federal departments and agencies remain in full force and effect. Additionally, this Plan does not confer additional authority on any Party, nor does it transfer or delegate authority to any party. This Plan is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

- This Plan recognizes the possibility of a cyber incident with physical impacts as well as a physical incident with cybersecurity implications. Accordingly, the Parties acknowledge a shared responsibility to enhance a national unity of effort in protecting critical infrastructure in both the cyber domain and physical realms by facilitating synchronization of information sharing, planning, and cyber response operations among the Parties. This approach will be executed consistent with law, policy, and regulation, including Executive Branch guidance expressed in EO 13636, *Improving Critical Infrastructure Cybersecurity*, Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, and PPD-41, *United States Cyber Incident Coordination*.

- The Parties agree to work together to leverage existing processes for States to request assistance from the appropriate Federal departments or agencies during a major cyber incident; requests are "requirements-based," and appropriate Federal authorities ultimately determine the Federal resources that are provided in support of SLTT authorities.

- This Plan will be implemented in a manner consistent with: Presidential Executive Orders and Policy Directives; the National Cybersecurity Strategy; the Department of Defense (DoD) Cyber Strategy; the Department of Homeland Security (DHS) Blueprint for a Secure Cyber Future; the Cybersecurity and Infrastructure Security Agency (CISA) Strategic Plan; Presidential Policy Directive 8, *National Preparedness*; the national planning frameworks; national strategic guidance on incident management and response; and other applicable laws and policies that assign roles, duties, and responsibilities to DHS/CISA, DoD, and other Federal departments and agencies to address strategic cybersecurity vulnerabilities, such as those affecting critical infrastructure, to develop robust cyber capabilities and partnerships, and to strengthen cybersecurity for intergovernmental, international, and critical industry partners.

- This Plan will be implemented consistent with the Emergency Management Assistance Compact and other interstate mutual aid agreements, such as the Pacific Northwest Emergency Management Accord, which facilitate the provision of State resources, including disaster recovery, law enforcement, and National Guard personnel and equipment under State command and control, from one or more supporting States to a supported State or States.
- This Plan will be implemented consistent with EO 13528 and the 2013 *State-Federal Consultative Process for Programming and Budgetary Proposals Affecting the National Guard*, and applicable State and Federal laws[ii] and policies.[iii]
- Improving and facilitating the shared situational awareness of emerging and current cybersecurity threats and vulnerabilities are critical to securing and defending Federal and SLTT interests.
- The Parties recognize that Federal and SLTT law enforcement agencies have an important role in cybersecurity that should be considered in activities undertaken pursuant to this Plan such as operational coordination, Federal assistance, and information-sharing activities.

IMPLEMENTATION

Authorities, roles, and responsibilities

- The Parties will collaborate on efforts to develop and periodically update lines of effort that promote a national approach to identify, protect against, detect, respond to, and recover from cyber incidents, including a national cyber incident response framework and other cyber incident management protocols and policies. In doing so, the Parties may consider the scope and applicability of existing authorities related to the prevention of, protection against, mitigation, response to, or recovery from cyber incidents and, as appropriate, identify areas of ambiguity or potential gaps in authority. This Plan recognizes that the Parties will ensure the protection of privacy, confidentiality, and civil rights and civil liberties consistent with applicable laws, regulations, and policies.

Planning

- The Parties will collaboratively exchange information on State and Federal requirements for cybersecurity to more fully inform discussions and ongoing efforts to build, sustain, and prioritize capabilities among all levels of government. This work will facilitate a discussion of how best to use or enhance existing State and Federal capabilities and authorities, including National Guard capabilities and Federal and State authorities related to the use of the National Guard, to address national surge capacity requirements.
- The Parties will develop a process to collaborate and discuss national-level and state-level cyber incident response planning, including national surge capacity.

- Consistent with the policy of the United States to have sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency, EO 12656, *Assignment of Emergency Preparedness Responsibilities*, assigns preparedness responsibilities to the heads of Federal departments and agencies during national security emergencies, and serves as an example of a useful planning tool that the Parties can reference during these incidents. As such, the Parties are encouraged to develop a collaborative process to incorporate tools such as EO 12656 and other authorities that address Federal roles and responsibilities during a cyber incident that is regarded as a national security emergency.

- The Parties will develop a process to collect and share after-action reports and lessons learned from cyber planning, activities, and exercises.

Mitigation and Resilience

- The Parties agree to work together to improve whole of community resilience and mitigate the potential effects of cyber incidents.

- CISA will work in collaboration with SLTT governments to enhance the cybersecurity posture of SLTT government organizations through near-real-time reporting and analysis, and as necessary, identify additional considerations to support the SLTT community effectively.

- The Parties will continue to support cybersecurity outreach and awareness efforts, including the National Initiative for Cybersecurity Education and promotion of Cyber Security Awareness Month.

- The Parties will work together to identify opportunities to: (1) address cybersecurity workforce challenges; (2) grow the cybersecurity talent pipeline; (3) promote cybersecurity education; and (4) explore the professionalization of cybersecurity careers through collaborative relationships and working groups.

Information Sharing

- The Parties agree that ascertaining accurate situational awareness of a developing cyber situation, emerging trends and threats, and the potential resultant cyber and physical effects is critical; therefore, DHS/CISA and SLTT governments will review and look for ways to increase the volume, timeliness, and quality of cyber threat information shared between DHS/CISA and SLTT government partners, leveraging efforts developed in response to EO 13636, PPD-21, and PPD-41.

- The Parties will encourage all SLTT partners to become members of the Multi-State Information Sharing and Analysis Center (MS-ISAC). The mission of the MS-ISAC is to improve the overall cybersecurity posture of SLTT government organizations through coordination, collaboration, cooperation, and increased communication. In addition, MS-ISAC develops, strategic, operational, and tactical

cybersecurity threat information, and advisories with actionable information to improve cybersecurity maturity and protections.

Operational Collaboration

- Arrangements for promoting unity of effort by SLTT and Federal entities undertaking actions to, identify, protect against, detect, respond to, and recover from cybersecurity incidents when those actions will directly or indirectly affect another party should be collaboratively developed and mutually agreed to by the Parties, to deconflict, synchronize, and enhance the effectiveness of security measures.
- The Parties agree to review, and to revise when needed, protocols and procedures to coordinate and deconflict actions undertaken in response to cybersecurity threats and, to the extent possible, avoid interference with law enforcement investigations of such cybersecurity incidents.

Public Information and Warning

- The Parties agree to continue the coordinated implementation of established protocols for delivering timely, coordinated, public information regarding cyber threats or incidents, consistent with applicable law and policies. The Parties agree to avoid interference with law enforcement investigations of such cybersecurity incidents.

REVIEW

- The Parties agree that this Plan should be reviewed annually to evaluate its effectiveness and that necessary changes will be made only through written amendments adopted with the consent of all the Parties.

Formally Adopted 2/2024

[i] "Response" is defined as "those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred," a definition derived from Presidential Policy Directive (PPD)-8, "National Preparedness."

[ii] Including U.S. Const. art II, section 2, cl. 1; section 113 of Title 10, U.S. Code; section 10102 of title 10, U.S. Code; section 7013 of title 10, U.S. Code; and section 9013 of title 10, U.S. Code.

[iii] Including DoD Directive 7045.14, *The Planning, Programming, Budgeting, and Execution (PPBE) Process*; DoD Instruction 8500.01, *Cybersecurity*; and Office of Management and Budget Circular A-11, *Preparation, Submission, and Execution of the Budget*.