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

The Council of Governors (Council) and its Federal participants (i.e., the Federal officials identified in Executive Order (EO) 13528 and officials of other Federal Executive departments or agencies as may be designated by the Secretary of Defense or the Secretary of Homeland Security) (i.e., "the Parties") adopt the following principles and actions for State-Federal unity of effort to strengthen the nation's security and resilience against cybersecurity threats. As adopted, this document forms a framework for establishing a collaborative environment for States, territories, and the Federal government to expedite and enhance the nation's response[1] to cyber incidents; improve cyber threat and vulnerability information sharing; utilize common capabilities and resources as appropriate, including the National Guard, to support State and Federal cyber missions; and secure and defend cyberspace, including State and Federal owned or operated critical infrastructure and key resources, in accordance with existing State and Federal laws and policies.

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

Principles

- The nation benefits when State and Federal entities fully utilize their authorities and resources in cooperation. This Joint Action 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 Declaration does not confer additional authority on any party, nor does it transfer authority to any party.

- This Joint Action Plan recognizes the possibility of a cyber incident with physical impacts as well as a physical incident with cyber implications. Accordingly, the Parties acknowledge a shared responsibility to enhance a national unity of effort in protecting critical infrastructure in both the cyber and physical realms by facilitating synchronization of information sharing, planning, and cyber response operations among the Parties. This approach will be executed consistent with existing law, policy, and regulation, including, but not limited to, Executive guidance expressed in EO 13636 and Presidential Policy Directive (PPD)-21.

- This Joint Action Plan recognizes that the Department of Homeland Security (DHS) works in close coordination with other agencies with complementary cyber missions, as well as private sector and other nonfederal owners and operators of critical infrastructure, to ensure greater unity of effort and a whole-of-nation response to cyber incidents. DHS coordinates

[1] "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-8, "National Preparedness."

the national protection against, mitigation of, and recovery from cyber incidents; works to prevent and protect against risks to critical infrastructure; disseminates domestic cyber threat and vulnerability analysis across critical infrastructure sectors; secures federal civilian systems; investigates, attributes, and disrupts cybercrimes under its jurisdiction; and coordinates federal government responses to significant incidents, whether cyber or physical, affecting critical infrastructure. The Department of Justice (DoJ) prosecutes cybercrimes; investigates, attributes, and disrupts cybercrimes under its jurisdiction; leads domestic national security operations regarding cyber threats, including disrupting foreign intelligence, terrorist, or other national security threats; and conducts domestic collection, analysis, and dissemination of cyber threat information. The Department of Defense (DoD) defends the nation from attack, secures national security and military systems, and gathers foreign cyber threat information.[2]

- This Joint Action Plan will be implemented in a manner consistent with existing Presidential Executive Orders and Policy Directives, the Department of Defense Strategy for Operating in Cyberspace, the Department of Homeland Security Blueprint for a Secure Cyber Future, 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, DoD, and other Federal departments and agencies to address strategic cyber vulnerabilities, such as those affecting critical infrastructure, development of robust cyber capabilities and partnerships, and efforts to strengthen cyber security for interagency, international, and critical industry partners.

- This Joint Action Plan will be implemented in a manner compatible with the existing Federal process in which requests for Federal assistance are "requirements-based" and appropriate Federal authorities ultimately determine the Federal resources that are provided in support of State and local authorities.

- This Joint Action 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.

- Consistent with EO 13528, *Establishing the Council of Governors*, and the 2013 *State-Federal Consultative Process for Programming and Budgetary Proposals Affecting the National Guard*, and other applicable State and Federal laws[3] and policies,[4] DoD and the

[2] 2014 Quadrennial Homeland Security Review.
[3] Including, but not limited to, 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 3103 of Title 10, U.S. Code; section 8103 of Title 10, U.S. Code.
[4] Including, but not limited to, DoD Directive 7045.14, DoD Instruction 8500.01, and OMB Circular A-11.

Council of Governors will continue to improve and clarify how views, information, or advice will be exchanged in advance (e.g., before formal submission of a proposed change) among the Parties on proposals for changing State or Federal laws, regulations, or policies, when such proposals would affect the roles and responsibilities of the National Guard in cyberspace in support of civil authorities.

- Improving and facilitating the shared situational awareness of emerging and current cyber threats and vulnerabilities are critical to securing and defending Federal, State, and local interests.

- The Parties recognize that State and Federal law enforcement have an important role in cybersecurity that should be considered in activities undertaken pursuant to this Joint Action Plan such as operational coordination, Federal assistance and information-sharing activities.

IMPLEMENTATION

Authorities, roles, and responsibilities

- Each Party will develop, enhance, and clarify policies, roles, and responsibilities that promote a national approach to preventing, protecting against, mitigating, responding to, and recovering from cyber incidents, including the development or refinement of a national cyber incident response framework and other cyber incident management protocols. In doing so, the Parties may consider the scope and applicability of existing authorities related to the prevention, protection against, mitigation, response to, or recovery from cyber incidents and, as appropriate, identify areas of ambiguity or potential gaps in authority. This Joint Action Plan recognizes that the Parties will ensure the protection of privacy, confidentiality, and civil rights and civil liberties consistent with applicable laws and policies.

- DoD, following the exchange of views, information, or advice with the Council of Governors, will update or, as necessary, establish DoD policy regarding State use of DoD cyber-related resources assigned to the National Guard.

Planning

- The Parties will collaboratively exchange views and information on State and Federal requirements for cybersecurity to inform more fully 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 but not limited to National Guard capabilities and authorities, to address national surge capacity requirements.

- DHS, in consultation with the Council of Governors, will develop a process to collaborate and discuss national-level and state-level cyber incident response planning and processes for collecting and sharing lessons learned from cyber planning and operations.

Mitigation and Resilience

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

- DHS and the States will work to enhance the cybersecurity posture of State, local, territorial, and tribal (SLTT) government organizations through near-real-time reporting and analysis, with efforts such as the Continuous Diagnostics and Mitigation program, and as necessary, identify additional considerations to support the SLTT community more effectively.

- The Parties will continue to support efforts of the National Initiative for Cybersecurity Education to promote public awareness of internet safety and security during National Cyber Security Awareness Month and the adoption of the Stop.Think.Connect.™ campaign. Additionally, the Parties will work together to identify opportunities to grow the cybersecurity talent pipeline, promote cybersecurity education, and 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, the Parties will review and look for ways to increase the volume, timeliness, and quality of cyber threat information between DHS and SLTT government partners, leveraging efforts developed in response to EO 13636 and PPD-21.

Operational Coordination

- Arrangements for promoting unity of effort by State and Federal entities undertaking actions to prevent, protect, mitigate, 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 establish protocols and procedures to coordinate and deconflict actions undertaken to counter 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, when appropriate, regarding any cyber threat or incident.

Federal Assistance

- 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.

REVIEW

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