AMENDMENT TO RULES COMM. PRINT 117–13
OFFERED BY MR. MOULTON OF MASSACHUSETTS

Add at the end of subtitle D of title XV of division A the following:

SEC. 15___. OPERATIONAL TECHNOLOGY AND MISSION-RELEVANT TERRAIN IN CYBERSPACE.

(a) MISSION-RELEVANT TERRAIN.—Not later than January 1, 2025, the Department of Defense shall have completed mapping of mission-relevant terrain in cyberspace for Defense Critical Assets and Task Critical Assets at sufficient granularity to enable mission thread analysis and situational awareness, including required—

(1) decomposition of missions reliant on such Assets;

(2) identification of access vectors;

(3) internal and external dependencies;

(4) topology of networks and network segments;

(5) cybersecurity defenses across information and operational technology on such Assets; and

(6) identification of associated or reliant weapon systems.

(b) COMBATANT COMMAND RESPONSIBILITIES.—Not later than January 1, 2024, the Commanders of United

States European Command, United States Indo-Pacific Command, United States Northern Command, United States Strategic Command, United States Space Command, United States Transportation Command, and other relevant Commands, in coordination with the Commander of United States Cyber Command, in order to enable effective mission thread analysis, cyber situational awareness, and effective cyber defense of Defense Critical Assets and Task Critical Assets under their control or in their areas of responsibility, shall develop, institute, and make necessary modifications to—

(1) internal combatant command processes, responsibilities, and functions;

(2) coordination with service components under their operational control, United States Cyber Command, Joint Forces Headquarters-Department of Defense Information Network, and the service cyber components;

(3) combatant command headquarters' situational awareness posture to ensure an appropriate level of cyber situational awareness of the forces, facilities, installations, bases, critical infrastructure, and weapon systems under their control or in their areas of responsibility, in particular, Defense Critical Assets and Task Critical Assets; and

(4) documentation of their mission-relevant terrain in cyberspace.

(c) DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER RESPONSIBILITIES.—

(1) IN GENERAL.—Not later than November 1, 2023, the Chief Information Officer of the Department of Defense shall establish or make necessary changes to policy, control systems standards, risk management framework and authority to operate policies, and cybersecurity reference architectures to provide baseline cybersecurity requirements for operational technology in facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network.

(2) IMPLEMENTATION OF POLICIES.—The Chief Information Officer shall leverage acquisition guidance, concerted assessment of the Department's operational technology enterprise, and coordination with the military department principal cyber advisors and chief information officers to drive necessary change and implementation of relevant policy across the Department's facilities, installations, bases, critical infrastructure, and weapon systems.

(3) ADDITIONAL RESPONSIBILITIES.—The Chief Information Officer shall ensure that policies,

control systems standards, and cybersecurity reference architectures—

(A) are implementable by components of the Department;

(B) in their implementation, limit adversaries' ability to reach or manipulate control systems through cyberspace;

(C) appropriately balance non-connectivity and monitoring requirements;

(D) include data collection and flow requirements;

(E) interoperate with and are informed by the operational community's workflows for defense of information and operational technology in facilities, installations, bases, critical infrastructure, and weapon systems;

(F) integrate and interoperate with Department mission assurance construct; and

(G) are implemented with respect to Defense Critical Assets and Task Critical Assets.

(d) UNITED STATES CYBER COMMAND OPERATIONAL RESPONSIBILITIES.—Not later than January 1, 2025, the Commander of United States Cyber Command shall make necessary modifications to the mission, scope, and posture of Joint Forces Headquarters-Department of

Defense Information Network to ensure that Joint Forces Headquarters—

(1) has appropriate visibility of operational technology in facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network and, in particular, Defense Critical Assets and Task Critical Assets;

(2) can effectively command and control forces to defend such operational technology; and

(3) has established processes for—

(A) incident and compliance reporting;

(B) ensuring compliance with Department of Defense cybersecurity policy; and

(C) ensuring that cyber vulnerabilities, attack vectors, and security violations, in particular those specific to Defense Critical Assets and Task Critical Assets, are appropriately managed.

(e) UNITED STATES CYBER COMMAND FUNCTIONAL RESPONSIBILITIES.—Not later than January 1, 2025, the Commander of United States Cyber Command shall—

(1) ensure in its role of Joint Forces Trainer for the Cyberspace Operations Forces that operational technology cyber defense is appropriately in-

corporated into training for the Cyberspace Operations Forces;

(2) delineate the specific force composition requirements within the Cyberspace Operations Forces for specialized cyber defense of operational technology, including the number, size, scale, and responsibilities of defined Cyber Operations Forces elements;

(3) develop and maintain, or support the development and maintenance of, a joint training curriculum for operational technology-focused Cyberspace Operations Forces;

(4) support the Chief Information Officer as the Department's senior official for the cybersecurity of operational technology under this section;

(5) develop and institutionalize, or support the development and institutionalization of, tradecraft for defense of operational technology across local defenders, cybersecurity service providers, cyber protection teams, and service-controlled forces; and

(6) develop and institutionalize integrated concepts of operation, operational workflows, and cybersecurity architectures for defense of information and operational technology in facilities, installations, bases, critical infrastructure, and weapon systems

across the Department of Defense Information Network and, in particular, Defense Critical Assets and Task Critical Assets, including—

(A) deliberate and strategic sensoring of such Network and Assets;

(B) instituting policies governing connections across and between such Network and Assets;

(C) modelling of normal behavior across and between such Network and Assets;

(D) engineering data flows across and between such Network and Assets;

(E) developing local defenders, cybersecurity service providers, cyber protection teams, and service-controlled forces' operational workflows and tactics, techniques, and procedures optimized for the designs, data flows, and policies of such Network and Assets;

(F) instituting of model defensive cyber operations and Department of Defense Information Network operations tradecraft; and

(G) integrating of such operations to ensure interoperability across echelons; and

(7) advance the integration of the Department of Defense's mission assurance, cybersecurity com-

pliance, cybersecurity operations, risk management framework, and authority to operate programs and policies.

(f) SERVICE RESPONSIBILITIES.—No later than January 1, 2025, the Secretaries of the military departments, through the service principal cyber advisors, chief information officers, the service cyber components, and relevant service commands, shall make necessary investments in operational technology in facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network and the service-controlled forces responsible for defense of such operational technology to—

(1) ensure that relevant local network and cybersecurity forces are responsible for defending and appropriately postured to defend operational technology across facilities, installations, bases, critical infrastructure, and weapon systems, in particular Defense Critical Assets and Task Critical Assets;

(2) ensure that relevant local operational technology-focused system operators, network and cybersecurity forces, mission defense teams and other service-retained forces, and cyber protection teams are appropriately trained, including through common training and use of cyber ranges, as appropriate, to

execute the specific requirements of cybersecurity operations in operational technology;

(3) ensure that all Defense Critical Assets and Task Critical Assets are monitored and defended by Cybersecurity Service Providers;

(4) ensure that operational technology is appropriately sensored and appropriate cybersecurity defenses, including technologies associated with the More Situational Awareness for Industrial Control Systems Joint Capability Technology Demonstration, are employed to enable defense of Defense Critical Assets and Task Critical Assets;

(5) implement Department of Defense Chief Information Officer policy germane to operational technology, in particular with respect to Defense Critical Assets and Task Critical Assets;

(6) plan for, designate, and train dedicate forces to be utilized in operational technology-centric roles across the military services and United States Cyber Command; and

(7) ensure that operational technology, as appropriate, is not easily accessible via the internet and that cybersecurity investments accord with mission risk to and relevant access vectors for Defense Critical Assets and Task Critical Assets.

(g) OFFICE OF THE SECRETARY OF DEFENSE RESPONSIBILITIES.—No later than January 1, 2023, the Secretary of Defense shall—

(1) assess and finalize Office of the Secretary of Defense components' roles responsibilities for the cybersecurity of operational technology in facilities, installations, bases, critical infrastructure, and weapon systems across the Department of Defense Information Network;

(2) assess the need to establish centralized or dedicated funding for remediation of cybersecurity gaps in operational technology across the Department of Defense Information Network and to drive implementation of this section;

(3) make relevant modifications to the Department of Defense's mission assurance construct, Mission Assurance Coordination Board, and other relevant bodies to drive—

(A) prioritization of kinetic and non-kinetic threats to the Department's missions and minimization of mission risk in the Department's war plans;

(B) prioritization of relevant mitigations and investments to harden and assure the De-

partment's missions and minimize mission risk in the Department's war plans; and

(C) completion of mission relevant terrain mapping of Defense Critical Assets and Task Critical Assets and population of associated assessment and mitigation data in authorized repositories;

(4) make relevant modifications to the Strategic Cybersecurity Program; and

(5) drive and provide oversight of the implementation of this section.

(h) BUDGET ROLLOUT BRIEFINGS.—

(1) Until January 1, 2024, at the annual staffer day briefings for the Committees on Armed Services of the Senate and the House of Representatives, each of the Secretaries of the military departments, the Commander of United States Cyber Command, and the Department of Defense Chief Information Officer shall provide updates on activities undertaken and progress made against the specific requirements of this section.

(2) No less frequently than annually until January 1, 2024, beginning no later than 1 year after the date of the enactment of this Act, the Under Secretary of Defense for Policy, the Under Secretary

of Defense for Acquisition and Sustainment, the Chief Information Officer, and the Joint Staff J6, representing the combatant commands, shall individually or together provide briefings to the Committees on Armed Services of the Senate and the House of Representatives on activities undertaken and progress made against the specific requirements of this section.

(i) IMPLEMENTATION.—

(1) IN GENERAL.—In implementing this section, the Department of Defense shall prioritize the cybersecurity and cyber defense of Defense Critical Assets and Task Critical Assets and shape cyber investments, policy, operations, and deployments to ensure cybersecurity and cyber defense.

(2) APPLICATION.—This section shall apply to assets owned and operated by the Department of Defense, as well as applicable, non-Department of Defense assets essential to the projection, support, and sustainment of military forces and operations worldwide.

(j) DEFINITION.—In this section, ''operational technology'' refers to control systems, or controllers, communication architectures, and user interfaces that monitor or control infrastructure and equipment operating in various

environments, such as weapons systems, utility or energy production and distribution, medical, logistics, nuclear, biological, chemical, and manufacturing facilities.

☒