

**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:

1 **SEC. 15 \_\_\_\_ . OPERATIONAL TECHNOLOGY AND MISSION-**  
2 **RELEVANT TERRAIN IN CYBERSPACE.**

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

9 (1) decomposition of missions reliant on such  
10 Assets;

11 (2) identification of access vectors;

12 (3) internal and external dependencies;

13 (4) topology of networks and network segments;

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

16 (6) identification of associated or reliant weap-  
17 on systems.

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

1 States European Command, United States Indo-Pacific  
2 Command, United States Northern Command, United  
3 States Strategic Command, United States Space Com-  
4 mand, United States Transportation Command, and other  
5 relevant Commands, in coordination with the Commander  
6 of United States Cyber Command, in order to enable effec-  
7 tive mission thread analysis, cyber situational awareness,  
8 and effective cyber defense of Defense Critical Assets and  
9 Task Critical Assets under their control or in their areas  
10 of responsibility, shall develop, institute, and make nec-  
11 essary modifications to—

12 (1) internal combatant command processes, re-  
13 sponsibilities, and functions;

14 (2) coordination with service components under  
15 their operational control, United States Cyber Com-  
16 mand, Joint Forces Headquarters-Department of  
17 Defense Information Network, and the service cyber  
18 components;

19 (3) combatant command headquarters' situa-  
20 tional awareness posture to ensure an appropriate  
21 level of cyber situational awareness of the forces, fa-  
22 cilities, installations, bases, critical infrastructure,  
23 and weapon systems under their control or in their  
24 areas of responsibility, in particular, Defense Critical  
25 Assets and Task Critical Assets; and

1           (4) documentation of their mission-relevant ter-  
2           rain in cyberspace.

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

5           (1) IN GENERAL.—Not later than November 1,  
6           2023, the Chief Information Officer of the Depart-  
7           ment of Defense shall establish or make necessary  
8           changes to policy, control systems standards, risk  
9           management framework and authority to operate  
10          policies, and cybersecurity reference architectures to  
11          provide baseline cybersecurity requirements for oper-  
12          ational technology in facilities, installations, bases,  
13          critical infrastructure, and weapon systems across  
14          the Department of Defense Information Network.

15          (2) IMPLEMENTATION OF POLICIES.—The Chief  
16          Information Officer shall leverage acquisition guid-  
17          ance, concerted assessment of the Department's  
18          operational technology enterprise, and coordination  
19          with the military department principal cyber advi-  
20          sors and chief information officers to drive necessary  
21          change and implementation of relevant policy across  
22          the Department's facilities, installations, bases, crit-  
23          ical infrastructure, and weapon systems.

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

1 control systems standards, and cybersecurity ref-  
2 erence architectures—

3 (A) are implementable by components of  
4 the Department;

5 (B) in their implementation, limit adver-  
6 saries' ability to reach or manipulate control  
7 systems through cyberspace;

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

10 (D) include data collection and flow re-  
11 quirements;

12 (E) interoperate with and are informed by  
13 the operational community's workflows for de-  
14 fense of information and operational technology  
15 in facilities, installations, bases, critical infra-  
16 structure, and weapon systems;

17 (F) integrate and interoperate with De-  
18 partment mission assurance construct; and

19 (G) are implemented with respect to De-  
20 fense Critical Assets and Task Critical Assets.

21 (d) UNITED STATES CYBER COMMAND OPER-  
22 ATIONAL RESPONSIBILITIES.—Not later than January 1,  
23 2025, the Commander of United States Cyber Command  
24 shall make necessary modifications to the mission, scope,  
25 and posture of Joint Forces Headquarters-Department of

1 Defense Information Network to ensure that Joint Forces  
2 Headquarters—

3 (1) has appropriate visibility of operational  
4 technology in facilities, installations, bases, critical  
5 infrastructure, and weapon systems across the De-  
6 partment of Defense Information Network and, in  
7 particular, Defense Critical Assets and Task Critical  
8 Assets;

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

11 (3) has established processes for—

12 (A) incident and compliance reporting;

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

15 (C) ensuring that cyber vulnerabilities, at-  
16 tack vectors, and security violations, in par-  
17 ticular those specific to Defense Critical Assets  
18 and Task Critical Assets, are appropriately  
19 managed.

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

23 (1) ensure in its role of Joint Forces Trainer  
24 for the Cyberspace Operations Forces that oper-  
25 ational technology cyber defense is appropriately in-

1        incorporated into training for the Cyberspace Oper-  
2        ations Forces;

3            (2) delineate the specific force composition re-  
4        quirements within the Cyberspace Operations Forces  
5        for specialized cyber defense of operational tech-  
6        nology, including the number, size, scale, and re-  
7        sponsibilities of defined Cyber Operations Forces ele-  
8        ments;

9            (3) develop and maintain, or support the devel-  
10        opment and maintenance of, a joint training cur-  
11        riculum for operational technology-focused Cyber-  
12        space Operations Forces;

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

16            (5) develop and institutionalize, or support the  
17        development and institutionalization of, tradecraft  
18        for defense of operational technology across local de-  
19        fenders, cybersecurity service providers, cyber pro-  
20        tection teams, and service-controlled forces; and

21            (6) develop and institutionalize integrated con-  
22        cepts of operation, operational workflows, and cyber-  
23        security architectures for defense of information and  
24        operational technology in facilities, installations,  
25        bases, critical infrastructure, and weapon systems

1 across the Department of Defense Information Net-  
2 work and, in particular, Defense Critical Assets and  
3 Task Critical Assets, including—

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

6 (B) instituting policies governing connec-  
7 tions across and between such Network and As-  
8 sets;

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

11 (D) engineering data flows across and be-  
12 tween such Network and Assets;

13 (E) developing local defenders, cybersecu-  
14 rity service providers, cyber protection teams,  
15 and service-controlled forces' operational  
16 workflows and tactics, techniques, and proce-  
17 dures optimized for the designs, data flows, and  
18 policies of such Network and Assets;

19 (F) instituting of model defensive cyber op-  
20 erations and Department of Defense Informa-  
21 tion Network operations tradecraft; and

22 (G) integrating of such operations to en-  
23 sure interoperability across echelons; and

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

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

4       (f) SERVICE RESPONSIBILITIES.—No later than Jan-  
5       uary 1, 2025, the Secretaries of the military departments,  
6       through the service principal cyber advisors, chief informa-  
7       tion officers, the service cyber components, and relevant  
8       service commands, shall make necessary investments in  
9       operational technology in facilities, installations, bases,  
10      critical infrastructure, and weapon systems across the De-  
11      partment of Defense Information Network and the serv-  
12      ice-controlled forces responsible for defense of such oper-  
13      ational technology to—

14               (1) ensure that relevant local network and cy-  
15               bersecurity forces are responsible for defending and  
16               appropriately postured to defend operational tech-  
17               nology across facilities, installations, bases, critical  
18               infrastructure, and weapon systems, in particular  
19               Defense Critical Assets and Task Critical Assets;

20               (2) ensure that relevant local operational tech-  
21               nology-focused system operators, network and cyber-  
22               security forces, mission defense teams and other  
23               service-retained forces, and cyber protection teams  
24               are appropriately trained, including through common  
25               training and use of cyber ranges, as appropriate, to



1 execute the specific requirements of cybersecurity  
2 operations in operational technology;

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

6 (4) ensure that operational technology is appro-  
7 priately sensed and appropriate cybersecurity de-  
8 fenses, including technologies associated with the  
9 More Situational Awareness for Industrial Control  
10 Systems Joint Capability Technology Demonstra-  
11 tion, are employed to enable defense of Defense Crit-  
12 ical Assets and Task Critical Assets;

13 (5) implement Department of Defense Chief In-  
14 formation Officer policy germane to operational  
15 technology, in particular with respect to Defense  
16 Critical Assets and Task Critical Assets;

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

21 (7) ensure that operational technology, as ap-  
22 propriate, is not easily accessible via the internet  
23 and that cybersecurity investments accord with mis-  
24 sion risk to and relevant access vectors for Defense  
25 Critical Assets and Task Critical Assets.

1 (g) OFFICE OF THE SECRETARY OF DEFENSE RE-  
2 SPONSIBILITIES.—No later than January 1, 2023, the  
3 Secretary of Defense shall—

4 (1) assess and finalize Office of the Secretary  
5 of Defense components' roles responsibilities for the  
6 cybersecurity of operational technology in facilities,  
7 installations, bases, critical infrastructure, and weap-  
8 on systems across the Department of Defense Infor-  
9 mation Network;

10 (2) assess the need to establish centralized or  
11 dedicated funding for remediation of cybersecurity  
12 gaps in operational technology across the Depart-  
13 ment of Defense Information Network and to drive  
14 implementation of this section;

15 (3) make relevant modifications to the Depart-  
16 ment of Defense's mission assurance construct, Mis-  
17 sion Assurance Coordination Board, and other rel-  
18 evant bodies to drive—

19 (A) prioritization of kinetic and non-kinetic  
20 threats to the Department's missions and mini-  
21 mization of mission risk in the Department's  
22 war plans;

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

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

3                   (C) completion of mission relevant terrain  
4           mapping of Defense Critical Assets and Task  
5           Critical Assets and population of associated as-  
6           sessment and mitigation data in authorized re-  
7           positories;

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

10           (5) drive and provide oversight of the imple-  
11           mentation of this section.

12           (h) BUDGET ROLLOUT BRIEFINGS.—

13                   (1) Until January 1, 2024, at the annual staff-  
14           er day briefings for the Committees on Armed Serv-  
15           ices of the Senate and the House of Representatives,  
16           each of the Secretaries of the military departments,  
17           the Commander of United States Cyber Command,  
18           and the Department of Defense Chief Information  
19           Officer shall provide updates on activities under-  
20           taken and progress made against the specific re-  
21           quirements of this section.

22                   (2) No less frequently than annually until Jan-  
23           uary 1, 2024, beginning no later than 1 year after  
24           the date of the enactment of this Act, the Under  
25           Secretary of Defense for Policy, the Under Secretary

1 of Defense for Acquisition and Sustainment, the  
2 Chief Information Officer, and the Joint Staff J6,  
3 representing the combatant commands, shall individ-  
4 ually or together provide briefings to the Committees  
5 on Armed Services of the Senate and the House of  
6 Representatives on activities undertaken and  
7 progress made against the specific requirements of  
8 this section.

9 (i) IMPLEMENTATION.—

10 (1) IN GENERAL.—In implementing this sec-  
11 tion, the Department of Defense shall prioritize the  
12 cybersecurity and cyber defense of Defense Critical  
13 Assets and Task Critical Assets and shape cyber in-  
14 vestments, policy, operations, and deployments to  
15 ensure cybersecurity and cyber defense.

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

22 (j) DEFINITION.—In this section, “operational tech-  
23 nology” refers to control systems, or controllers, commu-  
24 nication architectures, and user interfaces that monitor or  
25 control infrastructure and equipment operating in various

- 1 environments, such as weapons systems, utility or energy
- 2 production and distribution, medical, logistics, nuclear, bi-
- 3 ological, chemical, and manufacturing facilities.

