AMENDMENT TO RULES COMMITTEE PRINT 119–8

OFFERED BY MR. SUBRAMANYAM OF VIRGINIA

At the end of subtitle C of title XV, insert the following new section:

SEC. 15___. DATA RECOVERY REQUIREMENTS AND STRATEGY.

(a) DATA RECOVERY REQUIREMENTS.—Chapter 19 of title 10, United States Code, is amended by inserting after section 391b the following new section:

"§ 391c. Data recovery requirements

''(a) MANDATORY RECOVERY TIME OBJECTIVES.—

''(1) The Secretary of Defense shall, with respect to each element of the Department of Defense, carry out the following:

''(A) Designate essential data as one of the following types, as applicable:

''(i) Critical data.

''(ii) Important data.

''(iii) Necessary data.

''(B) Not later than 180 days after the date of the enactment of this section, establish

mandatory recovery time objectives for essential data so designated as critical data.

''(C) Not later than September 30, 2026, establish mandatory recovery time objectives for essential data so designated as important data or necessary data.

''(2) Each recovery time objective established under paragraph (1) shall satisfy the following requirements:

''(A) Be based upon the type of data to which such objective applies, including with respect to threat exposure.

''(B) Be updated in response to intelligence on evolving threats from state and non-state actors, including the People's Republic of China.

''(3) Not later than one year after the date of the enactment of this section and annually thereafter, the Secretary of Defense shall, for each element of the Department of Defense, submit to the congressional defense committees an auditable recovery certification report that includes information relating to the following:

''(A) Each recovery time objective that is established under paragraph (1) and applies to such element.

''(B) Whether such objective satisfies the requirements listed in paragraph (2).

''(b) DATA RECOVERY CAPABILITY REQUIREMENTS.—

''(1) Not later than 180 days after the date of the enactment of this section, the Secretary of Defense shall, for essential data designated as critical data pursuant to subparagraph (A) of subsection (a)(1), field data recovery capabilities that satisfy the following requirements:

''(A) Prioritize providing critical services in support of national defense.

''(B) Include the following:

''(i) Immutable backups that satisfy the following requirements:

''(I) Preserve logically separated copies of data.

''(II) Are selectively segmented or isolated from external networks by means of software, firewalls, or other controls.

''(ii) Continuous monitoring of backup environments to detect tampering, insider threats, and malicious corruption.

''(iii) Annual recovery exercises that simulate sophisticated nation-state cyberattacks designed to cripple data systems.

''(iv) Audits in which external or internal independent groups mimic tactics, techniques, and procedures of cyberattacks to assess and validate the ability of each element of the Department of Defense to carry out the objectives established under such subsection with respect to realistic threat conditions.

''(2) Not later than September 30, 2026, the Secretary of Defense shall, for essential data designated as important data or necessary data pursuant to subsection (a)(1)(A), field data recovery capabilities described in paragraph (1).

''(c) APPROVED TECHNOLOGY STANDARDS.—In fielding a data recovery capability under subsection (b), the Secretary of Defense may not adopt technology unless the following requirements are satisfied:

''(1) Such technology is listed in an inventory of the Department of Defense for certified cybersecurity and data protection technology.

''(2) If such technology is technology for recovering or repairing damaged or lost data, such technology provides for the following:

''(A) Immutable storage.

''(B) Robust recovery capabilities.

''(C) Full audit trails.

''(D) Continuous monitoring for data integrity and anomalous activity.

''(d) DEFINITIONS.—In this section:

''(1) The term 'critical data' means data, so vital to the United States, that the incapacity or destruction of such data would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof.

''(2) The term 'data recovery capability' means a technology, process, or governance framework to ensure rapid, secure, and verifiable recovery after a destructive cyberattack.

''(3) The term 'important data' means data that is important to the United States and the incapacity or destruction of such data would have a significant impact on security, national economic secu-

rity, national public health or safety, or any combination thereof.

''(4) The term 'necessary data' means data, the incapacity or destruction of which would have a measurable impact on security, national economic security, national public health or safety, or any combination thereof.

''(5) The term 'recovery time objective' means the maximum allowable time the Secretary of Defense determines necessary to restore critical functions and essential data following a cyberattack.''.

(b) DATA RECOVERY STRATEGY.—

(1) Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a data recovery strategy for the Department of Defense that includes information relating to the following:

(A) Recovery time objectives for such strategy.

(B) The technology necessary for such objectives.

(C) Oversight processes with respect to such strategy.

(D) The funds necessary to carry out such strategy.

(2) The strategy under paragraph (1) shall be submitted in unclassified form, but may contain a classified annex.

(3) In this subsection, the term ''recovery time objective'' means the maximum allowable time the Secretary of Defense determines necessary to restore critical functions and essential data following a cyberattack.