I

118TH CONGRESS
2D SESSION

H. R. 8775

To require an assessment on manual operations for critical infrastructure, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 18, 2024

Mr. CRENSHAW (for himself and Mr. MAGAZINER) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Transportation and Infrastructure, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To require an assessment on manual operations for critical infrastructure, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Contingency Plan for Critical Infrastructure Act''.

SEC. 2. ASSESSMENT ON MANUAL OPERATIONS FOR CRITICAL INFRASTRUCTURE.

(a) ASSESSMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security, in coordination with the Administrator of the Federal Emergency Management Agency (FEMA) and each sector risk management agency, shall provide to Congress a joint sector-by-sector assessment on the ability of critical infrastructure owners and operators to operate critical systems in a manual operating mode during cyber incidents.

(2) ELEMENTS.—The assessment under paragraph (1) shall include the following:

(A) An assessment of how the National Cyber Incident Response Plan (last published December 2016), accounts for the risk to critical infrastructure from not being able to rapidly transition into manually operating mode.

(B) An assessment of CISA's capabilities and responsibilities to not only remediate and respond to the digital aspects of cyber incidents, but to assist owners and operators of critical infrastructure to continue to operate key systems.

(C) An assessment of how FEMA's National Response Framework, including various Emergency Support Functions (ESFs) and Catastrophic Incident Response Teams (CIRT), are prepared to support owners and operators of critical infrastructure in events that require shifting to manual operating mode.

(D) An assessment of the potential costs and challenges associated with requiring sectors to be able to shift to manual operating mode in the event of a cyber incident.

(E) Policy recommendations to ensure continued operations of critical infrastructure in the event of a widespread cyber incident impacting critical infrastructure.

(b) UPDATED PLANNING CONSIDERATIONS FOR CYBER INCIDENTS.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Administrator of the Federal Emergency Management Agency, in coordination with the Director of the Cybersecurity and Critical Infrastructure Agency, shall update their Planning Considerations for Cyber Incidents (last published November 2023).

(2) ELEMENTS.—The updates required pursuant to paragraph (1) shall include the following:

(A) Best practices and guidelines for the essential personnel of critical infrastructure owners and operators to perform mission critical functions and continue to operate critical infrastructure in a manual operating mode during a cyber incident that disables business enterprise, process control, or communications systems.

(B) Steps that critical infrastructure owners and operators should take to respond to various levels of degradation to their systems to maintain operations.

(C) Identifying Federal, State, and local resources available to assist owners and operators of critical infrastructure in the event that a switch to manual operating mode is necessary.

(D) Specific guidelines on how to respond to and remediate the impact of cyber incidents on industrial control devices.

(c) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such

term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(2) MANUAL OPERATING MODE.—The term ''manual operating mode'' means a mode of operation with respect to critical infrastructure that is disconnected from the internet and with respect to which internal communication systems are degraded as a result of a cyber incident, but continues to allow such critical infrastructure to function to provide services to the public.

○