AMENDMENT TO THE RULES COMMITTEE PRINT FOR H.R. 4435 OFFERED BY MR. MCCAUL OF TEXAS

At the end of subtitle C of title XVI, add the following:

SEC. 1622. REAL-TIME INFORMATION SHARING CAPABILITY BETWEEN LEAD FEDERAL AGENCIES FOR CYBERSECURITY.

(a) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General, consistent with the protection of privacy and civil liberties, shall maintain the capability to provide shared situational awareness to the Department of Defense, the Department of Homeland Security, and the Department of Justice to enable real-time, integrated, and operational actions under each such department's respective authorities to protect from, prevent, mitigate, respond to, and recover from a cyber incident.

(b) DEFINITIONS.—In this section:

(1) SHARED SITUATIONAL AWARENESS.—The term ''shared situational awareness'' means an environment in which cyber threat information is shared

in real-time between the Department of Defense, the Department of Homeland Security, and the Department of Justice to provide actionable information relating to such cyber threat information.

(2) CYBER INCIDENT.—The term ''cyber incident'' means an incident, or an attempt to cause an incident, that, if successful, would—

(A) jeopardize or imminently jeopardize, without lawful authority, the security, integrity, confidentiality, or availability of an information system or network of information systems, or information stored on, processed on, or transiting such a system or network;

(B) constitute a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies related to such a system or network, or an act of terrorism against such a system or network; or

(C) result in the denial of access to or degradation, disruption, or destruction of such a system or network, or the defeat of an operations control or technical control essential to the security or operation of such a system or network.

(3) CYBER THREAT INFORMATION.—The term ''cyber threat information'' means information directly pertaining to—

(A) a vulnerability of an information system or network of information systems;

(B) a threat to the security, integrity, confidentiality, or availability of such a system or network, or any information stored on, processed on, or transiting such a system or network;

(C) efforts to deny access to or degrade, disrupt, or destroy such a system or network;

(D) efforts to gain unauthorized access to such a system or network, including to gain such unauthorized access for the purpose of exfiltrating information stored on, processed on, or transiting such a system or network; or

(E) an act of terrorism against an information system or network of information systems.

☒