Rubio-Feinstein *Sanction and Stop Ransomware Act of 2021*

Section-by-Section

Section 1
Short Title.

Section 2
Cybersecurity Standards for Critical Infrastructure. Critical infrastructure entity defined as an owner or operator of critical infrastructure

DHS Secretary with CISA Director shall develop cybersecurity standards for critical infrastructure entities. Standards to be consistent with existing federal regulations and incorporate existing NIST standards.

Compliance Assessment. At least annually the Secretary, in coordination with the heads of Sector Risk Management Agencies, shall assess compliance of each critical infrastructure entity with the standards developed.

Section 3
Regulation of Cryptocurrency Exchanges.

Directs the Secretary of Treasury, within 180 days, to develop and institute regulations for cryptocurrency exchanges operating in order to reduce anonymity of accounts and users suspected of ransomware activity and make records available to the US government in connection with ransomware incidents. Also directs the Secretary of Treasury to work with the Attorney General to determine what information is necessary for law enforcement.

The Secretary of Treasury will submit a report to Congress with recommendations to improve regulation of cryptocurrency exchanges in conjunction with ransomware.

Section 4
Designation of State Sponsors of Ransomware and Reporting Requirements.

Secretary of State, in consultation with the Director of National Intelligence (DNI), shall designate as a state sponsor of ransomware any country the government of which the Secretary has determined has provided support for ransomware demand schemes, including by providing safe haven for individuals or groups. List of such

countries shall be submitted to Congress 180 days after enactment, and annually thereafter.

The President shall impose sanctions and penalties on each state designated as a state sponsor of ransomware, consistent with sanctions and penalties levied on and against state sponsors of terrorism.

Within 180 days of enactment, the Secretary of Treasury shall submit a report to Congress that describes the numbers and geographic locations of individuals, groups, and entities subject to OFAC sanctions who were subsequently determined to have been involved in a ransomware demand scheme.

Secretary of State, with DNI and FBI Director, shall submit a report, both public and with classified annex, identifying the country of origin of foreign-based ransomware attacks.

Section 5
Deeming Ransomware Threats to Critical Infrastructure as a National Intelligence Priority.

Requires DNI, in consultation with FBI, to submit a report to intelligence committees on the implications of the ransomware threat to national security. The report shall identify individuals, groups, and entities posing ransomware threats; locations from where attacks occur; the infrastructure, tactics, and techniques used; relationships between ransomware actors and their governments that could negatively affect the ability of law enforcement to counter the threat of ransomware; and intelligence gaps needing attention.

Section 6
Ransomware Operation Reporting Capabilities.

CISA shall establish a system for a covered entity (federal contractor, owner or operator of critical infrastructure, non-government entity that provides cybersecurity incident response services, and any other entity determined appropriate by the Secretary). CISA shall receive ransomware operation notifications from other federal agencies and covered entities. Ransomware operation reporting system shall be established within 180 days. The CISA Director shall assess the system at least every two years and make any necessary corrective measures. Notifications submitted to the system shall be exempt from

FOIA disclosure and may not be admitted as evidence in any civil or criminal action or subject to subpoena except for from congress.

CISA director and secretary shall report annually to Congress on data from the reporting system.

Within 24 hours after the discovery of a ransomware operation, the federal agency or covered entity shall submit a notification to the system. The federal agency or covered entity must update the system as new information becomes available but not less frequently than every 5 days. The covered entity or federal agency is required to disclose any ransom payment including method, amount, and recipient.

Federal agencies and covered entities required to submit notifications obtain liability protections consistent with the Cybersecurity Act of 2015.

Penalties for non-compliance – removal from contracting schedules or inspector general referral as matter of urgent concern.

Section 7
Duties of CISA.

Establishes Information System and Network Security Fund for eligible entities; funds shall be made available to distribute for a specific network security purposes, including to enable network recovery from an event affecting the network cybersecurity of the eligible entity. Report required on use of funds. Eligible entity is a covered entity in compliance with the cybersecurity standards established under the bill. $1.5 billion authorized for 10 fiscal years.

Within 180 days, CISA director shall establish a public awareness campaign relating to cybersecurity services of the federal government. $10 million authorized for next 10 fiscal years.

Director may monitor the internet, including the dark web, for evidence of a compromise to critical infrastructure, and the Director shall develop, institute, and oversee capabilities to carry out this authority. If credible evidence of a compromise to critical infrastructure is identified, CISA shall notify the owner or operator as soon as is practicable.