IN THE CONGRESS OF THE UNITED STATES

MARCH 11th, 2022

Mr. MORALES (for himself) introduced the following bill;

To improve the cybersecurity of the Federal Government and to prepare for future cyberattacks.

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

Sec. 1. SHORT TITLE.

This act may be cited as the “Cybersecurity and Defense Act of 2022.”

Sec. 2. FINDINGS

Congress finds that—

(a) In November 2020, During the Elections, An attempted cyberattack in Madison, Wisconsin tried to interfere with the election by disrupting the power. During the same month, hackers cause a blackout by attacking the power grid and making the city of Madison go dark

(b) On March 10, 2022, The United States was hit with a massive cyberattack that targeted businesses and the United States Seventh Fleet.

Sec. 3. DEFINITIONS

In this act—

(a) The term "United States Cybersecurity and Infrastructure Security Agency" is a federal agency under the Department of Homeland Security oversight.

(b) The term "Ransomware" is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Sec. 4. ACTIVE CYBER DEFENSIVE STUDY

(a) After the enactment of this act, the Director of Cybersecurity and Infrastructure Security Agency shall perform a study on the use go active defense techniques to enhance the security of agencies, which shall include–

(1) A review of legal restrictions on the use of different active cyber defense techniques in Federal environments, in consultation with the Department of Justice

(2) The development of a framework for the use of different active defense techniques by agencies.

Sec. 5. RANSOMWARE THREAT

(a) Joint Ransomware Task Force.—

(1) IN GENERAL.— After the enactment of this act, The Attorney General and the Director of the Federal Bureau of Investigation shall establish and chair the Joint Ransomware Task Force to coordinate an ongoing nationwide campaign against ransomware attacks and identify and pursue opportunities for international cooperation.

(2) COMPOSITION.— The Joint Ransomware Task Force shall consist of participants from Federal agencies, as determined appropriate by the Secretary of Homeland Security.

(3) RESPONSIBILITIES.— The Joint Ransomware Task Force, utilizing only existing authorities of each participating Federal agency, shall coordinate across the Federal Government by the following activities:

(A) Prioritization of intelligence-driven operations to disrupt specific ransomware actors.

(B) Consult with the relevant private sector, State, local, tribal, and territorial governments, and international stakeholders to identify needs and establish mechanisms for providing input into the Joint Ransomware Task Force.

(C) Disrupting ransomware, criminal actors, associated infrastructure, and their finances.

(D) Facilitating coordination and collaboration between Federal entities and relevant entities, including the private sector, to improve Federal actions against ransomware threats.

(E) Collection, sharing, and analysis of ransomware trends to inform Federal actions.

Sec. 6. CODIFYING VULNERABILITY DISCLOSURE PROGRAMS

(a) Purpose

(1) PURPOSE.— The purpose of Federal vulnerability disclosure programs is to create a mechanism to use the expertise of the public to provide a service to Federal agencies by identifying information system vulnerabilities.

Sec. 7. MOBILE SECURITY STANDARDS

(a) IN GENERAL. After the enactment of this act, the Director shall–

(1) Evaluate mobile application security guidance by the Director; and

(2) Issue guidance to secure mobile devices, including for mobile applications for every agency.

Sec. 8. ENACTMENT

The provisions of this statute shall go into effect immediately upon the signature of the President.