SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON , DC 20301 - 1000

JANUARY 2021

CLASSIFIED: TOP SECRET - NOT FOR PUBLIC RELEASE

SUBJECT: RUSSIAN HACKINGS OF FEDERAL GOVERNMENT ASSETS

Throughout 2020, the United States received intelligence that Russian hackers have infiltrated secure government databases and servers, including those located in The Pentagon, the Intelligence Community, the US Treasury, the Department of Homeland Security, the Commerce Department, and Health and Human Services. Within the servers affected, 18,000 US organizations had malicious code in their networks; 50 of them suffered major breaches. As of the 13th of December, when this knowledge was made known to US officials, the Cybersecurity and Infrastructure Security Agency (CISA) has been working tirelessly to secure networks and alleviate any vulnerabilities in the systems that were affected. Russia has denied responsibility for such hackings.

This hacking poses a major threat to US cybersecurity, as it is one of the most significant hackings in modern history. The Department of Defense, Homeland Security, and CISA have urged Congress to take action against this emerging threat. In response, Congress has introduced the following piece of legislation, named after an essential cybersecurity tool: A Bill to C.A.P.T.C.H.A. (Create a Procedure to Combat Hacker Attacks). It is your responsibility as Congress to come to a decision on this legislation before more damage is done.

Christopher C. Miller
Acting

SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON , DC 20301 - 1000

JANUARY 2021

CLASSIFIED: TOP SECRET - NOT FOR PUBLIC RELEASE

SUBJECT: RUSSIAN HACKINGS OF FEDERAL GOVERNMENT ASSETS

Throughout 2020, the United States received intelligence that Russian hackers have infiltrated secure government databases and servers, including those located in The Pentagon, the Intelligence Community, the US Treasury, the Department of Homeland Security, the Commerce Department, and Health and Human Services. Within the servers affected, 18,000 US organizations had malicious code in their networks; 50 of them suffered major breaches. As of the 13th of December, when this knowledge was made known to US officials, the Cybersecurity and Infrastructure Security Agency (CISA) has been working tirelessly to secure networks and alleviate any vulnerabilities in the systems that were affected. Russia has denied responsibility for such hackings.

This hacking poses a major threat to US cybersecurity, as it is one of the most significant hackings in modern history. The Department of Defense, Homeland Security, and CISA have urged Congress to take action against this emerging threat. In response, Congress has introduced the following piece of legislation, named after an essential cybersecurity tool: A Bill to C.A.P.T.C.H.A. (Create a Procedure to Combat Hacker Attacks). It is your responsibility as Congress to come to a decision on this legislation before more damage is done.

A Bill to C.A.P.T.C.H.A. (Create A Procedure To Combat Hacker Attacks)

BE IT ENACTED BY THE CONGRESS HERE ASSEMBLED THAT:

SECTION 1. A. $10 billion shall be allocated to the Cybersecurity and Infrastructure Security Agency (CISA).

B. The Department of Defense shall award a separate Joint Enterprise Defense Infrastructure (JEDI) cloud computing contract to Amazon Web Services. The current JEDI contract with Microsoft shall not be terminated or overlap with Amazon Web Services' contract.

C. All departments and agencies of the US Federal Government must submit their cybergrids and defense mechanisms to audit and create a plan to address any discovered flaws.

D. US military and intelligence assets shall conduct small-scale, coordinated hackings of Russian government assets and servers to create offensive capability and parity with Russian hackers and cyberspace agents.

SECTION 2. A. JEDI shall be defined as a United States Department of Defense cloud computing contract awarded to private entities in order to enhance United States cybersecurity intelligence.

B. The Department of Defense and Intelligence Community have discretion to determine the scale and extent of the hackings of Russian assets.

SECTION 3. The Department of Defense and the Department of Homeland Security shall oversee the implementation of this legislation.

SECTION 4. This legislation shall be implemented immediately upon passage.

SECTION 5. All laws in conflict with this legislation are hereby declared null and void.

Introduced for Congressional Debate by The Sunvitational Security Team