Congress of the United States
Washington, DC 20515
January 28, 2021

The Honorable General Paul M. Nakasone
Director
National Security Agency
9800 Savage Rd., Suite 6272
Ft. George G. Meade, MD 20755

Dear General Nakasone:

We write to seek information about the National Security Agency's (NSA) role in the development of an encryption algorithm that leading cryptography experts say contains a backdoor. Years later, this backdoored encryption algorithm was exploited as part of a supply-chain hack, exposing the private data of corporate and U.S. government customers of Juniper Networks.

In 2006, the National Institute of Standards and Technology (NIST), which issues U.S. government standards for encryption algorithms, standardized Dual_EC_DRBG, an algorithm that produces random numbers, which are essential for secure encryption. As a senior NIST cryptographer subsequently confirmed in a public post-mortem, this algorithm was actually created by NSA, and given to NIST to publish as a government standard.

Although independent encryption experts had warned for years that the algorithm likely contained a backdoor that could be used to decrypt data, NIST dismissed the criticism, after being told by NSA that it had designed the algorithm in a "secure, classified way." According to the NIST cryptographer's post-mortem, NSA told NIST the algorithm "was originally intended for the national security community" and that the main reason for seeking NIST standardization was so that equipment used by federal agencies could be certified to government standards.

In essence, NSA told NIST that it created the algorithm for government use and that the concerns of non-governmental experts didn't matter, because companies that offered technology products to the general public didn't have to use it. The NSA-designed algorithm still ended up in hundreds of different technology products sold to American consumers, businesses, and non-profit organizations. This included internet routers and firewalls designed by Juniper, a U.S.-based networking technology company.

Sometime between 2008 and 2009, Juniper added the algorithm to several of its products. Juniper made this change secretly, which it kept from the public until 2013. In response to a recent congressional investigation, the company confirmed that it added support for the algorithm "at the request of a customer," but refused to identify that customer or even confirm whether that customer was a U.S. government agency. According to Juniper, no one involved in the decision to use this algorithm still works for the company.

In 2015, Juniper publicly revealed that it had learned of a major breach of its systems. The company discovered that in 2012, hackers broke into Juniper's servers and made a small modification to the code for the algorithm. This modified code was then incorporated by Juniper into security updates and new products. In essence, the hackers changed the key to the pre-existing backdoor that experts had long warned about in the algorithm— the backdoor remained, but now under the control of the unknown hackers.

Juniper has stated that it believes it was the victim of a hack by a foreign government. It also confirmed that the change to the code made by the hackers in 2012 could be exploited to decrypt customer data. This means that for approximately three years, a sophisticated adversary, possibly a foreign government, likely controlled a backdoor in Juniper's products which could be used to decrypt communications to or from the many U.S. business and government agencies that were using Juniper's products.

The Juniper hack may have caused immense harm to U.S. national security, although Congress and the public will likely never find out how much U.S. data was ultimately decrypted and exploited by our adversaries and the harm caused by the loss of this information. Congress has a responsibility to determine the root cause of this supply chain compromise and the NSA's role in the design and promotion of the flawed encryption algorithm that played such a central role. Moreover, the American people have a right to know why NSA did not act after the Juniper hack to protect the government from the serious threat posed by supply chain hacks. A similar supply chain hack was used in the recent SolarWinds breach, in which several government agencies were compromised with malware snuck into the company's software updates. To that end, please provide us with unclassified answers to the following questions by Februrary 26, 2021:

1. After Juniper's 2015 public disclosure that it inadvertently delivered software updates and products to customers containing malicious code, what actions did NSA take to protect itself, the Department of Defense, and the U.S. government from future software supply chain hacks? For each action, please identify why it was not successful in preventing the compromise of numerous government agencies in 2020 by a malware-laden update delivered by SolarWinds.
2. In the summer of 2018, during an unclassified briefing with Senator Wyden's office, senior NSA officials revealed the existence of a "lessons learned" report on the Dual_EC_DRBG algorithm. Senator Wyden's office has repeatedly requested this report, but NSA has yet to provide it. Please provide us with a copy of this report and any official historical reports that describe this algorithm, its development, and subsequent exploitation.
3. At the time that NSA submitted Dual_EC_DRBG to NIST for certification, did NSA know the algorithm contained a backdoor?
4. According to the NIST cryptographer's postmortem, NSA informed NIST in 2005 that it selected the "Q" value that was published in the NIST Duel_EC_DRBG standard in a "secure, classified way." Was this statement accurate? Please explain.
5. Juniper has confirmed that it added support for Dual_EC_DRBG "at the request of a customer," but refused to identify that customer, or even confirm whether that customer was a U.S. government agency. Did NSA request that Juniper include in its products the

Dual_EC_DRBG algorithm, P and Q values which were different from those published by NIST, or another NSA-designed encryption standard named Extended Random?

6. What statutory legal authority, if any, would permit NSA to introduce vulnerabilities into U.S. government approved algorithms certified by NIST and to keep those vulnerabilities hidden from NIST?
7. Would efforts by NSA to introduce backdoors or other vulnerabilities into government standards require the approval of the NSA Director, an inter-agency consultation, including input from the Cybersecurity and Infrastructure Security Agency, the Department of Commerce, the Federal Trade Commission, and the Federal Communications Commission? Would they require notification to the Congressional intelligence committees or an order from the Foreign Intelligence Surveillance Court? If no, please explain why.

Thank you for your attention to this important matter.

Sincerely,

Ron Wyden
United States Senator

Cory A. Booker
United States Senator

Tom Malinowski
Member of Congress

Pramila Jayapal
Member of Congress

Ted W. Lieu

Ted W. Lieu
Member of Congress

Stephen F. Lynch
Member of Congress

Bill Foster

Bill Foster
Member of Congress

Suzan K. DelBene
Member of Congress

Yvette D. Clarke M.C.

Yvette D. Clarke
Member of Congress

Anna G. Eshoo
Member of Congress