

# United States Senate

WASHINGTON, DC 20510

July 26, 2023

Dr. Kelly Fletcher  
Chief Information Officer  
U.S. Department of State  
Harry S. Truman Building  
2201 C Street NW  
Room 6311  
Washington, DC 20520

Dr. Fletcher,

Safeguarding our national security and domestic secrets from foreign adversaries is the utmost priority for our government. We were recently made aware that senior officials within the U.S. Department of State and various other Departments were victims of a People's Republic of China (PRC)-backed cyber-attack, which resulted in compromised email accounts. It was reported that Chinese cyber-spies exploited a fundamental gap in the State Department's cloud-based security architecture that provided broad access to sensitive electronic communications between senior officials.

In recent years, China has committed increasingly brazen and frequent acts of cyber-espionage. The PRC is singularly focused on using its advanced hacking program to acquire sensitive information, especially from the United States. Using a blend of state and non-state actors, China has sought to gain access to information systems across the U.S. Federal Government. Cyber-espionage originating from China has increased significantly, and will continue to do so. U.S. federal agencies must take the necessary steps to secure their networks and better mitigate against attacks. It is crucial those in the executive, federal, and legislative branch are confident the only people reading their emails are the intended recipients—not our adversaries.

As the United States Senate continues to evaluate legislation and proposals which shore up both immediate and long-term threats across U.S. government information systems, timely information related to the recent cyber-intrusions into the State Department's network is critical. We request accurate information from your Department related to the cyber-espionage operations purportedly conducted by China's state-sponsored cyber-espionage group, Storm-0558, against State Department Information Systems. Please address the following questions in a closed, unclassified briefing available to members and their staff:

1. Which State Department officials were compromised during Storm-0558's cyberespionage campaign?
2. We are told the State Department discovered the cyber-espionage operation as a result of

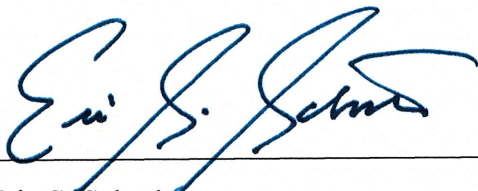
a gap in the cloud-based security provider's security architecture. After notifying the cloud-based security provider of the breach, when was a security patch provided to mitigate ongoing and future attacks?

3. What steps are you taking to ensure future sophisticated attacks are mitigated? Do you anticipate needing additional tools to support this effort?

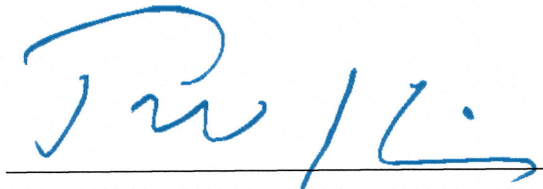
4. How will this recent cyber-intrusion shape the State Department's potential \$10 billion Evolve IT initiative? How will you ensure a more robust, layered cybersecurity architecture that includes multiple cybersecurity vendors for unclassified email?

The response to these questions should be provided no later than September 6, 2023.

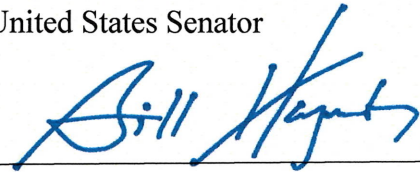
Sincerely,



Eric S. Schmitt  
United States Senator



Tim Kaine  
United States Senator



Bill Hagerty  
United States Senator



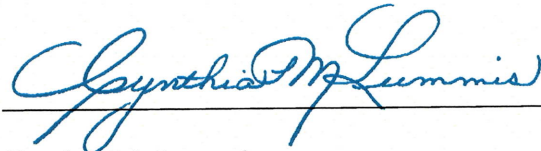
Ben Cardin  
United States Senator



Mike Braun  
United States Senator



Josh Hawley  
United States Senator



Cynthia M. Lummis  
United States Senator



J.D. Vance  
United States Senator



---

Katie Britt  
United States Senator



---

Rick Scott  
United States Senator



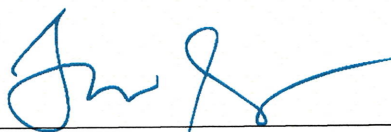
---

Mark Kelly  
United States Senator



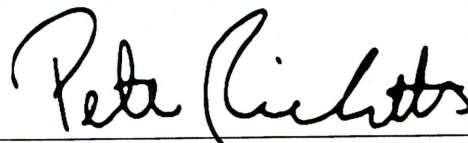
---

John Barrasso, M.D.  
United States Senator



---

Tim Scott  
United States Senator



---

Pete Ricketts  
United States Senator