

# United States Senate

WASHINGTON, DC 20510

September 11, 2018

The Honorable Mike Pompeo  
Secretary of State  
U.S Department of State  
Washington, D.C 20520

Dear Secretary Pompeo:

We write in response to reports from federal auditors that the Department of State is failing to meet federal cybersecurity standards. We urge you to improve compliance by enabling more secure authentication mechanisms across the Department of State's information systems.

For much of the Internet's history, users have been prompted to enter passwords to access their email and other online accounts. This password-only approach is no longer sufficient to protect sensitive information from sophisticated phishing attempts and other forms of credential theft. Indeed, many organizations have turned to multi-factor authentication (MFA), a security technology requiring users to provide multiple "factors" to gain access to a system or network. These can take the form of biometric data, secondary digital devices, or short codes. While certainly not a silver bullet, MFA is a simple step that makes it significantly harder for foreign governments or criminals to access accounts.

According to a 2018 General Service Administration (GSA) assessment of federal cybersecurity, the Department of State had only deployed enhanced access controls across 11% of required agency devices. This despite a law—the Federal Cybersecurity Enhancement Act—requiring all Executive Branch agencies to enable MFA for all accounts with "elevated privileges." Similarly, the Department of State's Inspector General (IG) found last year that 33% of diplomatic missions failed to conduct even the most basic cyber threat management practices, like regular reviews and audits. The IG also noted that experts who tested these systems "successfully exploited vulnerabilities in email accounts of Department personnel as well as Department applications and operating systems."

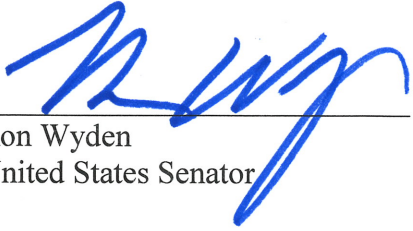
We are sure you will agree on the need to protect American diplomacy from cyber attacks, which is why we have such a hard time understanding why the Department of State has not followed the lead of many other agencies and complied with federal law requiring agency use of MFA. To help us better understand the state of play, please respond to the following questions by October 12, 2018:

1. What actions has the Department of State taken in response to the OMB's designation of the Department of State's cyber readiness as "high risk"?
2. What actions has the Department of State taken to rectify the near total absence of multifactor authentication systems for accounts with elevated privileges accessing the agency's network, as required by federal law?

3. Please provide us with statistics, for each of the past three years, detailing the number of cyber attacks against Department of State systems located abroad. Please include statistics about both successful and attempted attacks.

Thank you for your prompt attention to this matter.

Sincerely,



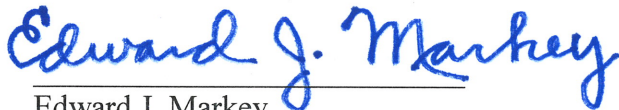
---

Ron Wyden  
United States Senator



---

Cory Gardner  
United States Senator



---

Edward J. Markey  
United States Senator



---

Rand Paul  
United States Senator



---

Jeanne Shaheen  
United States Senator