MARK R. WARNER
VIRGINIA

COMMITTEES:
FINANCE
BANKING, HOUSING, AND URBAN AFFAIRS
BUDGET
INTELLIGENCE
RULES AND ADMINISTRATION

United States Senate

WASHINGTON, DC 20510–4606

January 14, 2020

The Honorable Mike Pompeo
Secretary of State
U.S. Department of State
2201 C Street NW
Washington, DC 20520

Dear Secretary Pompeo:

As tensions between the United States and Iran rise, and the risks of Iran carrying out cyberattacks with "disruptive effects" grow, I write to express my deep concern about the State Department's ability to defend its information security systems and that of our embassies around the world, and request a plan for how you will bolster these systems.[1]

The Iranian government's state-sponsored cybersecurity capabilities have grown in sophistication and intensity in recent years, and they have developed a number of advanced persistent threat (APT) groups that conduct various offensive operations. Examples include prolonged espionage, destructive malware and ransomware attacks, and social media manipulation through influence campaigns. These attacks serve both political and economic purposes, and use methods like password spray attacks, scanning for VPN vulnerabilities, DNS hijacking, spear-phishing emails, and social engineering. Iran's threat group APT33 has been linked to notorious disk-wiping malware including SHAMOON and SHAPESHIFT (which attacked industrial systems across the Middle East and in Europe). As recently as 2018, the Department of Justice indicted two Iranian men for deploying ransomware to extort hospitals, municipalities, and public institutions, causing over $30 million in losses.[2]

In August 2019, the Department of State's Office of Inspector General (OIG) issued a report on the effects of the hiring freeze on the State Department, finding in particular, serious impacts on the cybersecurity functions of the Department. The IG found the following:

> The bureau was unable to fill two Senior Executive Service positions responsible for cybersecurity, which it said delayed implementing an enterprise risk management program for IT systems. The DS [Bureau of Diplomatic Security] Computer and Technical Security Directorate reported that staffing shortfalls hampered its ability to develop tools and procedures to react and respond to malicious cyber activity targeting Department personnel and information assets. DS also reported delays in conducting penetration testing of Department networks and providing IT security support for

[1] "DHS Issues Bulletin Warning of Potential Iranian Cyberattack," by Maggie Miller, *The Hill*, Jan 6, 2020
[2] "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals, Municipalities, and Public Institutions, Causing Over $30 Million in Losses," Office of Public Affairs, U.S. Department of Justice, Nov 28, 2018

integrating cybersecurity for new and existing systems, which they attributed, in part, to the hiring freeze.[3]

That IG report followed a 2017 report by the State Department OIG that noted a number of cybersecurity risks presented by the structure of the State Department. The report noted that the Chief Information Security Officer was not well placed to be held fully accountable for State Department cybersecurity issues, and highlighted an incident in Guatemala City where unauthorized and misconfigured network devices comprised the Department's sensitive network.[4]

The State Department has a long history of information security breaches, beginning with a series of blunders in the late 1990's, and including a massive and prolonged attack in 2014, when the National Security Agency (NSA) and Russian hackers fought for control of State Department servers.[5] In September 2018, after an email breach of unclassified systems, a bipartisan group of Senators asked you how the State Department was addressing the issue.[6] Two months later, hackers with suspected ties to the Russian government were found to be impersonating State Department officials in an attempt to infiltrate computers belonging to the U.S. government, the military, and defense contractors.[7] In March 2019, a State Department contractor was convicted of theft and embezzlement of 16 computers from your organization.[8]

Given Iran's technical capabilities and threats to retaliate, as well as the State Department's systemic organizational and functional problems addressing cybersecurity vulnerabilities, I ask you to answer the following questions on how the State Department will address a surge of offensive cyber activity by Iran:

1. Currently, cybersecurity personnel are dispersed organizationally across different bureaus within the Department of State, and across embassies around the world. Since the OIG report was issued in August 2019, what personnel changes have you made to more efficiently and effectively address both the hiring freeze impacts and the earlier security and audit concerns presented by the OIG?

---

[3] "Review of the Effects of the Department of State Hiring Freeze," Office of Inspector General, U.S. Department of State, Aug 9, 2019

[4] *From the OIG Report, "Inspector General Statement on the Department of State's Major Management and Performance Challenges, FY 2018,"* "The inspection of Embassy Guatemala City detailed an example of the consequence of failure to comply with key procedures. OIG discovered that its Information Management Section staff installed unauthorized and misconfigured network devices on the Department's sensitive network, creating IT security vulnerabilities. From July through November 2017, the embassy reported three incidents involving unauthorized and misconfigured network devices, two of which OIG identified during this inspection. As a result, OIG recommended that DS, in coordination with IRM and Embassy Guatemala City, audit the embassy's sensitive network to ensure it complies with Department standards."

[5] "State Department Email Breach Exposed Employees' Personal Information," by Eric Geller and Nahal Toosi, *Politico*, Sep 17, 2018.

[6] Ibid.

[7] "Russian Hackers Said To Be Impersonating U.S. State Dept. With Phishing Campaign," by Robert Olsen, *Forbes*, Nov 20, 2018.

[8] "Former State Department Contractor Pleads Guilty to Stealing Computers," U.S. Attorney's Office, Eastern District of Virginia, U.S. Department of Justice, Mar 7, 2019.

2. The OIG report noted that the Chief Information Security Officer (CISO) of the Department of State lacked necessary seniority for effectiveness or accountability. My understanding is that the current CIO reports to the Undersecretary for Management to the Secretary of State, and that the CISO reports to the CIO. In 2018 a study by the Financial Services Information Sharing and Analysis Center (FS-ISAC) recommended that CISO's have clear and direct communication with the CEO, rather than just to the CIO.[9] Most organizations provide at least a dotted-line reporting structure from the CISO to the CEO. What kind of direct communication do you have with the CISO, given that the position sits below a CIO and an Undersecretary?
3. What kind of employee training changes have you made to protect employees from phishing and other social engineering attacks?
4. What technical changes have you made within the information security organization of the State Department to protect against ransomware and wiper malware attacks?
5. Have you addressed the August 2019 OIG report's hiring concerns for information and IT security personnel at our embassies? Are you up-to-date on your information security audits? Does the State Department, at the very least, conduct routine scanning, patching, and utilize multifactor authentication?

I would appreciate your answers by January 31, 2020.

Sincerely,

Mark R Warner

MARK R. WARNER
United States Senator

[9] "2018 CISO Cybersecurity Trends," Financial Services Information Sharing and Analysis Center, Feb 2018