

United States Senate

WASHINGTON, DC 20510

March 13, 2019

The Honorable Michael C. Stenger
Sergeant at Arms
United States Senate
Washington, D.C. 20530

Dear Mr Stenger:

We write to you today to ask that you disclose to each U.S. Senator the extent of the cyber threats faced by the U.S. Senate—and by extension, our democracy. This information is imperative in order to help the U.S. Senate address important cyber-security needs.

During the last decade, hackers have successfully infiltrated U.S. government agencies including the Office of Personnel Management, health care firms such as Anthem, and technology giants like Google. Hackers continue to target all manner of government entities, and there is little doubt that Congress is squarely in their sights. Indeed, as your predecessor testified before the U.S. Senate Committee on Appropriations in June 2017, “the Senate is considered a prime target for cybersecurity breaches.” The Sergeant at Arms must be transparent in providing members of the Senate all information about the possible existence and scale of successful hacks against the Senate.

In 2006, computers in the offices of then-Congressman Frank Wolf were hacked, reportedly originating from IP addresses in China. Speaking at a press conference in 2008, Congressman Wolf put the scale of the information theft in stark terms: “They got everything.” During a debate in 2008 over congressional cybersecurity—the one and only time the cybersecurity of the legislative branch has been openly debated on the floor of either chamber—Congressman Wolf remarked that “ever since this happened, I’ve been deeply concerned that this institution, the institution of the United States Congress, is definitely not adequately aware of, or protected from, these types of threats.”

The 2006 incident was not the only time the public learned that foreign hackers compromised Congressional computers—during an Armed Services Committee hearing in 2009, then-Senator Bill Nelson revealed that “I have had my office computers invaded three times in the last month, and one of them, we think, is very serious.” Later, Senator Nelson revealed at another hearing that his office’s compromised computer was discovered “talking to a computer in some international arena.”

According to media reports, Russian and Chinese hackers have in recent years breached the White House, Pentagon, State Department, and other agencies in the executive branch. Yet, the last publicly-disclosed breach of congressional computers was in 2009.

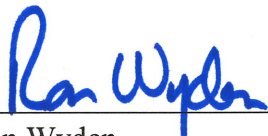
Companies and executive branch agencies are required by state and federal law to report breaches. In contrast, Congress has no legal obligation to disclose breaches and other cyber

incidents. We believe that the lack of data regarding successful cyber attacks against the Congress has contributed to the absence of debate regarding congressional cybersecurity—this must change. Each U.S. Senator deserves to know, and has a responsibility to know, if and how many times Senate computers have been hacked, and whether the Senate’s existing cybersecurity measures are sufficient to protect both the integrity of this institution and the sensitive data with which it has been entrusted.

We understand that details of specific incidents may need to remain confidential, however, providing Senators with aggregate statistics about successful cyber attacks would enable the Senate to engage in informed debate about the security threats faced by the legislative branch and consequently, the need for the Senate to fund, prioritize, and conduct aggressive oversight over its own cybersecurity. To that end, we ask that you take the following steps:

1. Provide each Senator, annually, with aggregate statistics revealing the number of cyber incidents in which:
 - a. Senate computers have been compromised; and
 - b. Hackers have otherwise gained access to sensitive Senate data.
2. Commit to a policy of informing Senate leadership and all of the members of the Senate Committees on Rules and Intelligence, within 5 days of discovery, of any breach of a Senate computer.

Sincerely,



Ron Wyden
United States Senator



Tom Cotton
United States Senator