

May 24, 2018

The Honorable Kirstjen M. Nielsen
Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Nielsen:

I write to request additional information on the voluntary cybersecurity assistance the Department of Homeland Security (DHS) provides to political campaigns.

As you know, political campaigns are attractive targets for foreign nations seeking to meddle in the American political process. Russia's coordinated efforts to influence the 2016 election clearly demonstrated that even well-financed presidential campaigns are vulnerable to cyberattacks. Many smaller campaigns will be completely unprepared to properly protect themselves.

In a previous letter, I urged DHS to designate political campaigns as critical infrastructure. Responding for DHS, Christopher C. Krebs indicated that DHS would provide voluntary cybersecurity assistance "to any political entity upon request." In a follow-up email with my office, Mr. Krebs stated that:

Political campaigns can contact the National Cybersecurity and Communications Integration Center (NCCIC) to report cybersecurity information or receive additional information about how they can engage with DHS on cybersecurity matters. NCCIC's website can be found here: <https://www.us-cert.gov/>. NCCIC can be reached by phone at: (888) 282-0870; or by email at: NCCICcustomerservice@hq.dhs.gov.

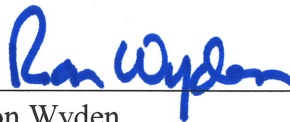
I commend DHS for confirming that it will provide cybersecurity assistance to political campaigns—but unless DHS advertises this voluntary service, campaigns are unlikely to utilize it. Campaigns must also understand the range of the technical expertise and strategic advice available to them so they can properly leverage DHS's technical assistance. To this end, I request that you provide answers to the following questions by June 22, 2018:

- What specific technical cybersecurity support and advice did DHS provide the Trump and Clinton presidential campaigns during the 2016 election?
- Has DHS provided cybersecurity-related assistance to any federal, state, or local campaigns in the 2018 election cycle?
 - If yes, to how many campaigns?

- If yes, what specific technical cybersecurity support and advice has DHS provided?
- How does DHS assess whether the cybersecurity assistance it gives to political campaigns is effective or successful?
- Did DHS make changes to the cybersecurity assistance it provides to campaigns or to the ways in which it provides that assistance following the 2016 election cycle?
 - If yes, please detail any changes that were made.
- At his recent confirmation hearing before the Senate Select Committee on Intelligence, I asked William Evanina, the nominee to be Director of the National Counterintelligence & Security Center, if government officials should encrypt their unclassified telephone communications. Mr. Evanina declared his firm belief that they should. Does DHS concur with Mr. Evanina's recommendation that government officials should encrypt their unclassified telephone conversations?
 - If yes, what steps, if any, has DHS taken to communicate these recommendations to federal agencies.
- Given the clear foreign intelligence threat faced by elected officials, including those running for elected office, does DHS currently advise political campaigns to use end-to-end encrypted apps like Signal to secure their calls and text messages?
 - If not, why not?

If you have any questions regarding this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator