

August 2, 2018

The Honorable Christopher C. Krebs
Under Secretary
National Protection and Program Directorate
Department of Homeland Security
Washington, D.C. 20528

Dear Mr. Krebs:

I am writing to you today to better understand what the Department of Homeland Security (DHS) has learned from Domain-based Message Authentication, Reporting and Conformance (DMARC) reports about hackers, scammers, and other malicious actors using email to impersonate federal agencies—otherwise known as email spoofing.

In October 2017, at my urging, DHS issued Binding Operational Directive 18-01, which mandates that civilian agencies utilize a number of cybersecurity best practices. These include a requirement that civilian agencies enable DMARC, a technology designed to detect and prevent spoofing of email messages by causing the transmission of reports to DHS whenever a suspicious email spoofing a federal agency is sent. Since January 14, 2018, civilian agencies have been required to enable automatic DMARC reporting to DHS, giving DHS an unparalleled, government-wide perspective on efforts by malicious actors to impersonate federal agencies. Agencies have until October 16, 2018 to enable a more restrictive DMARC mode which will cause emails impersonating those agencies to be automatically rejected by many large email providers, such as Google and Yahoo.

However, requiring agencies to transmit email impersonation threat data to DHS is only the first step. DHS must then collate and analyze those reports in order to understand the scope of the threat and to determine how best to protect federal agencies from impersonation. Indeed, in my July 18, 2017 letter to DHS, I urged DHS to create a central system to receive and process DMARC reports from agencies across the government.

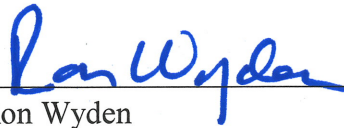
DHS has received DMARC reports from federal agencies for more than six months. Accordingly, I would like to understand what steps DHS has taken to analyze this information and to turn it into actionable cyber intelligence. To that end, I would appreciate answers to the following questions by August 31, 2018:

1. Which civilian agencies have yet to enable the automatic transmission of DMARC reports to DHS?
2. How is DHS analyzing the DMARC reports? Please describe any challenges, if any, the agency has encountered in analyzing this data.

3. What actionable cyber intelligence has DHS distilled from these reports?
4. How has DHS analysis enabled agencies to authenticate their email infrastructure and move towards a DMARC 'reject' policy, as they are required to do by October 16, 2018?
5. Does DHS provide DMARC analytic capabilities to state, local, tribal, and territorial governments? 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