

July 18, 2017

Jeanette Manfra
Senior Official Performing the Duties of the Under Secretary
National Protection & Programs Directorate
Department of Homeland Security
Washington, D.C. 20528

Dear Ms. Manfra:

I write to ask you to take immediate steps to ensure that hackers cannot send emails that impersonate federal agencies. Industry-standard technologies exist, and are already used throughout the private sector and even by a few federal agencies, which, if enabled, would make it significantly harder for fraudsters and foreign governments to impersonate federal agencies.

The threat posed by criminals and foreign governments impersonating U.S. government agencies is real. For example, in May, news reports revealed an active phishing campaign in which hackers were sending emails purporting to come from the Defense Security Service. Likewise, in 2016, the Internal Revenue Service reported a 400% increase in attempts by criminals to impersonate the agency through phishing.

In 2015, the information technology industry finalized a technical standard known as Domain-based Message Authentication, Reporting & Conformance (DMARC). This technology enables agency administrators to request that fake email messages impersonating that organization be quarantined in a spam folder, or rejected by a recipient's email provider. I write to you today to ask that the Department of Homeland Security (DHS) use its authority under the Federal Information Security Modernization Act to mandate that federal agencies adopt this cybersecurity technology, which will prevent fraudsters from being able to send emails that purport to come from .gov domains.

Other federal cyber security leaders such as the National Institute for Standards and Technology (NIST) and Federal Trade Commission (FTC) strongly recommend DMARC. A few federal agencies, including the FTC, the Federal Deposit Insurance Corporation, and the Social Security Administration have taken the initiative by enabling DMARC. Moreover, they have configured it in the most strict "reject" mode so that email service providers can automatically reject phishing emails impersonating their agency. Unfortunately, most agencies, including DHS, have still not enabled DMARC or configured it in the strongest setting.

Government-wide implementation of DMARC has had a huge impact in the United Kingdom. In 2016, the U.K. required all government agencies to enable DMARC. As a result, the U.K.'s tax agency has stated that it reduced the number of phishing emails purporting to come from that

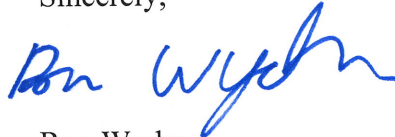
agency by a staggering 300 million messages in one year. In addition to mandating the use of DMARC, the U.K. government's National Cyber Security Centre (NCSC) also created a central system to receive and process DMARC reports from all government agencies. Importantly, the NCSC now has cross-government visibility into efforts by adversaries to impersonate any of the more than 100 U.K. government domains currently feeding reports into the system.

It is time for the U.S government to adopt DMARC. To that end, I ask that DHS promptly take the following steps:

1. DHS scans federal agencies systems for known cybersecurity vulnerabilities as part of the Cyber Hygiene program. Please add DMARC scanning to this program.
2. Work with the General Services Administration to create a central system, similar to the service offered by the U.K. NCSC, to receive automatic DMARC reports from federal agencies across the government.
3. Issue a Binding Operational Directive requiring executive branch agencies to enable DMARC with a reject or quarantine policy. Further mandate that agencies configure their DMARC reports to be sent to the central reporting system operated by DHS, so that DHS has visibility into any efforts by criminals and foreign governments to impersonate U.S. government agencies.

If you have any questions about this request, please contact Anderson Heiman on my staff at (202) 224-4515.

Sincerely,



Ron Wyden
United States Senator

CC: Rob Joyce, White House Cybersecurity Coordinator