DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

JUL 20 2018

Senator Ron Wyden
United States Senate
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for your letter on May 22, 2018 concerning the cybersecurity of Department of Defense (DoD) public-facing websites and services. Secretary Mattis outlined three lines of effort within the National Defense Strategy for the Department of Defense: rebuilding military readiness to build a more lethal force, strengthening alliances to attract new partners, and reforming the Department's business practices for greater performance and affordability. Rapidly deploying the trust-related cybersecurity capabilities listed in the letter, in conjunction with Federal, Allied, and business mission partners, is consistent with the DoD CIO's charge to support the Secretary's objectives.

The Department has already been working for several years on the web and email security measures identified in the inquiry. Onboarding these capabilities has included infrastructure refresh and adjustments to policy over the last 2-3 years. The Department is working hard to ensure DoD inspires trust among citizens and partners in its digital interactions across our missions, business, and entitlements roles.

The culmination of this significant preparation and mission analysis will be a Joint Force Headquarters-DoD Information Network (JTF-DoDIN) Task Order that implements the cybersecurity measures contained in Department of Homeland Security Binding Operational Directive (BOD) 18-01 under DoD authorities. The Department will provide a copy of this Task Order, which is targeted for release by August 17, 2018. Enclosed is the DoD plan for implementing the measures included in the BOD with a target completion date of December 31, 2018 for everything but full implementation of HSTS which requires more testing. A roll out plan for HSTS will be released by December 31, 2018.

DoD takes pride in being a leader in cyberspace and supports the need to protect information, both for the warfighter as well as the general public. DoD will monitor the Task Order implementation to ensure DoD public facing web-sites and services remain secure.

Sincerely,

Dana Deasy

Enclosure:
As stated

Department of Defense (DoD) Activities to Secure Public Facing Web and Email Services

DoD is working with United States Cyber Command (CYBERCOM) and Joint Force Headquarters – DoD Information Networks (JFHQ-DoDIN) to finalize direction under DoD authorities to implement each of the measures contained in Binding Operational Directive (BOD) 18-01. The action plan below identifies planning target dates, pending ongoing mission analysis. Dates may change in the final task order but all tasks other than full HSTS deployment will be completed by December 31, 2018.

Public Trust Public Key Infrastructure (PKI)

- The Department has leveraged the "direct trust" model using its own PKIs for many years but this has proven to be a challenge with our external partners. DoD will issue direction to implement commercial publicly trusted certificates on DoD's public-facing sites and services while we complete work on the Federal/DoD public trust PKI.
    - Planning target of October 31, 2018 for completion.
    - Majority of DoD components are already employing commercial certificates for their public facing websites.
        - CIO issued policy allowing commercial EV certificates in February 14, 2017 for public-facing sites; this was revised in January 5, 2018 to allow DV certificates.
        - Extended Validation certificates provided additional proofing and vetting, but DoD approved Domain Validation certificates after determining that the assurance of DoD's Domain Name Service management processes provided comparable assurance without the additional cost.
        - For example, the Defense Media Agency (DMA), which operates many of DOD's public information resources, including the DOD-CIO public site, began deploying publicly-trusted certificates on sites they operate in mid-January 2018 and complete all sites by August 31, 2018.
- Pivoting toward a "public-trust" model began as a long-term effort; DoD and the Federal Government are now within 18 months of completion.
    - For the longer-term solution, DoD has been aggressively working with Federal partners for almost two years to significantly improve the trust experience for consumers and partners by participating in the "Public Trust" Federal Public Key Infrastructure (FPKI) root cooperative effort between DoD and General Services Administration, along with other Federal stakeholders. Short lived machine generated certificates will be part of this capability.
    - It is anticipated that the "public trust" root and issuing certificate authorities, as well as supporting certificate transparency services, will be completed by

December 31, 2018.

  - o It will likely take another full year (December 31, 2019) for the various commercial trust store operators (e.g. Microsoft, Google) to integrate the FPKI root into their trust stores.

- DoD will also direct elimination of weak ciphers and encryption with a planning target of September 30, 2018 for completion.

HSTS Preload

- Although HSTS can assure the use of HTTPS, it can have negative impacts such as denial-of-service on sub-domains or improperly prepared root domains. Once committed to using HSTS preload, there is no quick "rollback" option. DoD also needs to conduct thorough testing to ensure that our "break and inspect" capabilities are not hampered by the implementation of HSTS Preload.

- In the interim, DoD will issue direction to prepare for implementation of HSTS preload for domains within the .mil hierarchy and work to address any issues potentially created with the Department's defensive capabilities.

- DoD will direct that all public facing websites are to use HTTPS, regardless of HSTS Preload state, and authorize the use of HSTS on DoD web sites that are ready. This direction will also include the requirement for all HTTP requests to redirect to HTTPS.

- JFHQ-DoDIN and DoD CIO will continue to work with each DoD Component head in preparation for the use of HSTS and engage with DHS on the processes to utilize the HSTS Preload list feature for DoD domains. A roll out plan for HSTS will be issued December 31,2018

STARTTLS and DMARC

- Today, there are several organizations and companies with whom DoD already use STARTTLS as either being required or preferred.

- DoD will issue direction to implement STARTTLS and DMARC on all DoD mail servers in two phases.

- The initial phase will include DOD's mail servers that are supported by DISA-operated Enterprise Email Messaging Security Gateway (EEMSG). Preparation for this phase began in 2017 with refreshment of hardware and software to support these capabilities at the EEMSG. The planning target for completion of this phase is July 2018 for STARTTLS PREFERRED, and August 2018 for inbound DMARC. This phase includes most DoD email servers and email accounts.

- The second phase will include implementation of STARTTLS PREFERRED and inbound DMARC for all DoD email servers that are not behind the EEMSG, and configuration of outbound DMARC for all DoD mail servers. The planning target for this phase is completion by December 2018.

- DoD continues to execute its plans to implement STARTTLS and DMARC for the DoD Enterprise. These preparations were underway for some time.

- DoD will continue to implement STARTTLS REQUIRED over time in coordination with other mail providers; ensuring that both providers agree that failure to establish an encrypted session will result in mail not being delivered and that processes are in place to address potential failures.