Homeland Security

Office of Cybersecurity and Communications
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

MEMORANDUM FROM THE ASSISTANT SECRETARY

TO: Agency POC
Agency

SUBJECT: **Temporary Policy Exception for BOD 18-01 Action Related to Disabling the Weak Email Cipher 3DES**

In reference to Binding Operational Directive 18-01: *Enhance Email and Web Security*, issued on October 16, 2017 to all Federal agencies, the Department of Homeland Security (DHS) is hereby issuing a temporary policy exception on the BOD requirement related to disabling the weak email cipher 3DES. Based on discussions with Federal agency leaders and industry representatives, DHS acknowledges that there is a significant constraint around disabling the weak email cipher 3DES. This constraint relates to current industry timelines and vendor expectations associated with the use of 3DES. Though DHS has observed progress in this area over the past year, we have determined that many agencies are dependent upon email service providers to make necessary changes in order for the agency to comply with the BOD 18-01 requirement for disabling the weak email cipher 3DES.

As a result, DHS is granting a temporary exception to agencies that have notified DHS of a known vendor constraint with respect to disabling weak email ciphers until the agency's respective email vendor provides options for disabling the weak email cipher 3DES. DHS will continue to work with the vendor community to determine when 3DES can be effectively disabled for email communications by each specific vendor or provider. Once such action is feasible, DHS will formally notify applicable agencies of the new requirement and timeline. At that time, applicable agencies must ensure the weak email cipher 3DES are disabled within 30 calendar days to fully comply with BOD 18-01 requirements. Disabling of weak ciphers on web servers under BOD 18-01 remains an active requirement that is not impacted by this exception.

In order for your agency to receive the temporary exception from disabling weak email ciphers, your agency must submit an updated Plan of Action and Milestones that includes the following:

- The vendor causing the constraint,
- The estimated timeline for disabling the weak email cipher 3DES, if known,
- The preventative security measures and mitigation strategy that will be put in place while accepting risk.

Jeanette Manfra
Assistant Secretary
Office of Cybersecurity & Communications
Department of Homeland Security

Sept 20, 2018
Date