CHIEF INFORMATION OFFICER

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

DEC 2 3 2022

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS

SUBJECT: Department of Defense Transition to Stronger Public Key Infrastructure Algorithms

References:
(a) National Institute of Standards and Technology Special Publication 800-57 Part I, Revision 5, dated May 2020
(b) Committee on National Security Systems Policy 15, dated October 20, 2016

This memorandum provides guidance to the Department of Defense (DoD) components on actions they must undertake as DoD migrates to stronger algorithms for the DoD and National Security Systems (NSS) Public Key Infrastructures (PKI). The DoD Non-classified Internet Protocol Router Network (NIPRNet) and NSS Secret Internet Protocol Router Network (SIPRNet) PKI currently use the Rivest, Shamir and Adelman (RSA)-2048 cryptographic algorithm and the Secure Hash Algorithm (SHA)-256 in order to perform operations and keep communications secure.

The DoD will cease issuing PKI certificates utilizing RSA-2048 and SHA-256 on both NIPRNet and SIPRNet on 31 December 2027. The DoD will transition the DoD NIPRNet and NSS SIPRNet PKIs to algorithms and key sizes compliant with the National Security Agency's Commercial National Security Algorithm Suite 2.0. The DoD NIPRNet and NSS SIPRNet PKIs will transition to using at least RSA-3072 (4096 is preferred) and SHA-384 cryptographic algorithms.

In order to issue PKI credentials with stronger algorithms, DoD information technology infrastructure (e.g., server and workstation operating systems, browsers, and e-mail applications) must be capable of supporting these stronger algorithms. Accordingly, the DoD CIO directs the following for both the NIPRNet and SIPRNet:

- Effective immediately, all Public Key enabled commercial-off-the-shelf software and Public Key enabled Open-Source software integrations performed or purchased either as new procurements or as part of scheduled and budgeted DoD Component technology refreshes and upgrades (on both NIPRNet and SIPRNet) must support at least RSA-3072 (4096 is preferred) and SHA-384. Systems that will sunset before December 2027 are exempt from this requirement.

- All DoD information systems that have been upgraded or are upgrading to support RSA-3072 (or RSA-4096) and SHA-384 must continue to maintain backward compatibility with DoD's current RSA-2048/SHA-256 PKI credentials.

- If a DoD Component system is regularly accessed by federal or industry partners as part of its mission, the system owner is strongly encouraged to work with those partners to coordinate algorithm upgrade plans so as to limit interoperability difficulties.

- If a DoD Component cannot ascertain from a vendor whether a product is at least RSA-3072 (4096 is preferred) and SHA-384 compatible, the Component should contact its representative at the Test and Evaluation Working Group (TEWG) or the SIPRNet Token Evaluation Working Group (STEWG). The TEWG (CACsupport@mail.mil) will coordinate testing of vendor products to determine compatibility with RSA-4096 and SHA-384 on the NIPRNet, and the STEWG (PKI_Test_Team@nsa.gov) will coordinate testing of vendor products on the SIPRNet.

- RSA-3072 (and RSA-4096) and SHA-384 product compatibility information can be found on the DoD Cryptographic Modernization page, which is located on a PKI protected webpage of the DISA Cyber.mil website (https://cyber.mil/pki-pke/cryptographic-modernization/).

To transition to these stronger algorithms, both the NIPR and SIPR PKIs will require new card stock. The DoD CIO anticipates that new card stock will be available by the end of Fiscal Year (FY) 2026. DoD Component Program Objective Memoranda (POM) should account for the complete replacement of all on-hand and in-use NIPRNet and SIPRNet card stock based on anticipated card issuance for the period of FY 2027 through FY 2030.

The Office of the DoD CIO will coordinate with the Office of the Under Secretary of Defense for Acquisition and Sustainment and United States Cyber Command to codify the above activity within the Department's acquisition and cyber operation communities. My point of contact is [redacted].

John B. Sherman