CHIEF INFORMATION OFFICER

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

DEC 01 2015

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEFS OF MILITARY SERVICES
COMMANDANT OF THE UNITED STATES COAST GUARD
COMMANDERS OF THE COMBATANT COMMANDS
CHIEF OF THE NATIONAL GUARD BUREAU
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, OPERATIONAL TEST AND EVALUATION
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Revised Schedule to Update DoD Public Key Infrastructure Certificates to Secure Hash Algorithm-256

References: DoD CIO Memorandum, “DoD Secure Hash Algorithm-256 Transition Plan,” July 18, 2013

This memorandum revises the schedule for transitioning DoD Common Access Card (CAC) Public Key Infrastructure (PKI) certificates and Non-classified Internet Protocol Router Network (NIPRNet) software certificates from Secure Hash Algorithm (SHA)-1 to SHA-256.

Recent cybersecurity events have required DoD to harden its networks at an accelerated pace. The Reference directed DoD to support SHA-256 by September 30, 2017, and to start issuing SHA-256 CACs by October 1, 2018. The schedule for issuing NIPRNet SHA-256 PKI certificates that was established in the Reference is hereby rescinded. It is replaced by the schedule in the Attachment to this memorandum. A new schedule for issuing Secret Internet Protocol Router Network (SIPRNet) SHA-256 certificates has not yet been established.

The point of contact is Mr. David Lassen, david.lassen2.civ@mail.mil, 703 614-2137.

Terry A. Halvorsen

Attachment:
As stated

ATTACHMENT

The DoD Components, the Defense Information Systems Agency (DISA), the Defense Manpower Data Center (DMDC), and the United States Cyber Command (USCYBERCOM) are directed to take the actions described in the schedule below:

November 2015

- DISA will install SHA-256 CAC certificate authorities (CAs) in production and make them available for DMDC testing.
- DISA and USCYBERCOM will notify DoD Components of the new NIPRNet CAs and trust chains.
- DoD Components will begin updating certificate trust stores on NIPRNet devices with the new CAC CAs.

December 2015 (Date in Reference was September 30, 2017)

- DoD Components will complete updating certificate trust stores on NIPRNet devices with the new SHA-256 software CAs and the DoD Root 3 CA.
- SHA-256 Software CAs will be available for issuing software certificates.

January 2016

- DoD Components will begin issuing only SHA-256 Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and code signing certificates, and begin replacing SHA-1 SSL/TLS and code signing certificates with SHA-256 certificates (with limited exceptions).

March 2016

- DoD Components will complete updating certificate trust stores on NIPRNet devices with the new CAC CAs.
- DISA will disable SHA-1 SSL/TLS certificate profiles on issuing CAs on March 1, 2016.

April 2016 (Date in Reference was October 1, 2018)

- DMDC will begin issuing SHA-256 CACs, and DoD Components will begin issuing Alternate Logon Tokens with SHA-256 certificates.

December 2016

- DoD Components will complete replacing SHA-1 SSL/TLS and code signing certificates with SHA-256 certificates.

April 2019 (Date in Reference was September 30, 2020)

- All active CACs in circulation will have SHA-256 certificates.