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

CHIEF INFORMATION OFFICER

OCT - 4 2018

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: Update to Department of Defense Chief Information Officer Memorandum on Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites

This memorandum updates and replaces DoD Chief Information Officer (CIO) Memorandum, "Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites," January 5, 2018. It provides clarification on where commercial certificates may be purchased and expands the policy for use of commercial certificates on DoD Mobile Device Management (MDM) systems.

Most commercial web browsers and operating systems do not explicitly trust DoD Public Key Infrastructure (PKI) certificates. This results in external users receiving an untrusted certificate message when trying to access DoD public facing websites. DoD and the Federal PKI program office are working together to implement a joint PKI which will be trusted by most widely-used commercial web browsers and operating systems. This should be available within the next 18 months. Until this capability is fully implemented, DoD Components may use commercial Secure Socket Layer device certificates in accordance with the attached criteria. Commercial device certificates may be installed on unclassified public-facing DoD websites and unclassified DoD MDM systems. DoD Components may also use commercial code-signing certificates to certify code on their websites.

This memorandum will remain in effect for two years from the date it is signed. The DoD CIO retains the discretion to modify the memorandum's terms and conditions, as well as its effective term. The point of contact for this matter is Mr. Andy Seymour at: (571) 372-6990, charles.a.seymour.civ@mail.mil.

Dana Deasy

Attachment:
As stated

DISTRIBUTION:
Chief Management Officer of the Department of Defense
Secretaries of the Military Departments
Chairman of the Joint Chiefs of Staff
Under Secretaries of Defense
Chiefs of the Military Services
Chief, National Guard Bureau
Commandant of the Coast Guard
Commanders of the Combatant Commands
General Counsel of the Department of Defense
Director of Cost Assessment and Program Evaluation
Inspector General of the Department of Defense
Director of Operational Test and Evaluation
Assistant Secretary of Defense for Legislative Affairs
Assistant to the Secretary of Defense for Public Affairs
Director of NET Assessment
Directors of the Defense Agencies
Directors of the DoD Field Activities

ATTACHMENT

Criteria required for the use of commercial certificates: (DoD websites and services not conforming to this criteria must not use commercial device or code signing certificates.)

- Systems hosted on a Defense Information System Network, must be hosted in a DoD demilitarized zone.

- Only commercial device and code signing certificates from external PKI vendors listed on the Defense Information Systems Agency's Information Assurance Support Environment at: http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx may be used.

- Certificates must use the Secure Hash Algorithm (SHA)-256 or a stronger hash algorithm (Requests to vendors must specify SHA-256 certificates should be issued under a SHA-256 Root Certificate Authority).

- Websites operated in the *.gov* and *.mil* top level domain space, must ensure the commercial device and/or code signing PKI certificates at minimum meet the criteria for Domain Validation.