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

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

SUBJECT: Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites

This memorandum extends and replaces DoD Chief Information Officer (CIO) Memorandum, "Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites," November 8, 2021. It clarifies the circumstances and criteria where commercial PKI certificates may be issued to DoD Non-Person Entities (NPE) and used for code-signing.

Most commercial web browsers, operating systems, and mail servers do not trust DoD Public Key Infrastructure (PKI) certificates. This causes external users to receive an untrusted certificate message when trying to access DoD public facing websites. It also makes it difficult to encrypt internet traffic between DoD and non-DoD mail servers. The DoD CIO is working with the Federal PKI on an alternative PKI solution which will be trusted by most commercial web browsers, operating systems, and mail servers.

For one year after the date of this memorandum, DoD Components may install Transport Layer Security (TLS) NPE PKI certificates issued by a commercial PKI on unclassified DoD websites, Mobile Device Management (MDM) systems, and Enterprise Email Message Security Gateway (EEMSG) mail servers, provided that the criteria in Attachment A are met. DoD Components may also use code-signing PKI certificates issued by a commercial PKI to certify code on their unclassified DoD websites, provided that the criteria in Attachment A are met.

Per Attachment B, the Defense Media Activity (DMA) has been granted a limited and conditional exemption to one of the criteria in Attachment A.

The DoD CIO retains the discretion to modify the memorandum's terms and conditions, as well as its effective period. The point of contact for this memorandum is Colonel Silas J. Calhoun, (571) 372-4594, silas.j.calhoun.mil@mail.mil or osd.mc-alex.dod-cio.mbx.icam@mail.mil.

BHATIA.GURPREET.SINGH.1298222171

Digitally signed by BHATIA.GURPREET.SINGH.1298222171
Date: 2022.12.16 09:53:21 -05'00'

Gurpreet S. Bhatia
Principal Director, Deputy Chief Information Officer for Cybersecurity

Attachment:
As Stated

ATTACHMENT A: CRITERIA

Criteria for Issuing Commercial NPE PKI Certificates to DoD websites, MDM systems, and EEMSG mail servers:

1. The DoD website or EEMSG mail server must be unclassified and public facing. The public-facing requirement is not applicable to MDM systems.

2. If the DoD website, MDM system, or EEMSG mail server is hosted on a defense information system network, then it must be hosted in an appropriately isolated network segment (e.g., a DoD de-militarized zone).

3. If the DoD website, MDM system, or EEMSG mail server operates in the .gov or .mil top-level domain space, the commercial PKI certificate must meet the criteria for domain validation.

4. The commercial NPE PKI certificate must use the Secure Hash Algorithm (SHA) 256 or a stronger hash algorithm and must be issued under a SHA-256 root Certificate Authority (CA).

5. The commercial NPE PKI certificate must be issued by either a vendor that also operates a DoD-approved external PKI listed on the DoD cyber exchange PKI interoperability website at https://cyber.mil/pki-pke/interoperability, or a vendor that is also an External Certification Authority (ECA) vendor listed on the DoD cyber exchange ECA website at https://cyber.mil/eca/.

Criteria for Commercial Code-Signing PKI Certificates:

1. The DoD website must be unclassified and public facing.

2. If the DoD website is hosted on a defense information system network, then it must be hosted in an appropriately isolated network segment (e.g., a DoD de-militarized zone).

3. If the DoD website operates in the .gov or .mil top-level domain space, the commercial PKI certificate must meet the criteria for domain validation.

4. The commercial code-signing PKI certificate must use the SHA-256 or a stronger hash algorithm and must be issued under a SHA-256 root CA.

5. The commercial code-signing PKI certificate must be issued by either a vendor that also operates a DoD-approved external PKI listed on the DoD cyber exchange PKI interoperability website at https://cyber.mil/pki-pke/interoperability, or a vendor that is also an ECA vendor listed on the DoD cyber exchange ECA website at https://cyber.mil/eca/.

ATTACHMENT B: DEFENSE MEDIA ACTIVITY

Let's Encrypt is a non-profit PKI vendor which does not meet the fifth criteria for commercial PKI certificates on NPEs, as it is not a vendor that also operates a DoD-approved external PKI listed on the DoD cyber exchange PKI interoperability website, and it is not a vendor that is also an ECA vendor listed on the DoD cyber exchange ECA website. Per the DoD CIO Memorandum "Limited Approval for Defense Media Activity's Use of the Let's Encrypt Public Key Infrastructure for Public Information Websites," September 2020, the Defense Media Activity (DMA) may install Let's Encrypt NPE PKI certificates on their NPEs provided that:

- DMA follows all of the other criteria in Attachment A for issuing commercial PKI certs to NPE.

- DMA only uses Let's Encrypt NPE PKI certificates, and does not accept any other types of PKI certificates issued by Let's Encrypt.

- DMA only installs the Let's Encrypt NPE PKI certificates on systems, servers, and websites that are unclassified, publicly facing, and publicly accessible.

- DMA protects data sensitivity by only using Let's Encrypt NPE PKI certificates for Cloud Computing Impact Level (IL) 2 data and below, per the DoD Cloud Computing Security Requirements Guide.

- DMA employs the Automatic Certificate Management Environment (ACME) protocol as the means of maintaining NPE PKI certificates for Let's Encrypt.

- Let's Encrypt maintains its PKI cross-certification with IdenTrust.

Under no circumstances may any other DoD Component aside from DMA issue, use, or install Let's Encrypt PKI certificates, or any other commercial PKI which does not comply with the criteria in Attachment A, without express written approval from the DoD CIO or the Deputy DoD CIO for Cybersecurity.