DoD Instruction 8520.02

Public Key Infrastructure and Public Key Enabling

Originating Component:	Office of the DoD Chief Information Officer
Effective:	May 18, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	John B. Sherman, DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance:

- Establishes policy, assigns responsibilities, and prescribes procedures for DoD public key infrastructure (PKI) and public key enabling (PKE).
- Provides procedures for:
  - Developing and implementing a DoD PKI to enhance the security of DoD information systems (ISs) by enabling systems to use PKI for authentication, digital signatures, and encryption.
  - DoD PKI and PKE activities on DoD unclassified networks, DoD Secret Fabric networks, and networks within the DoD Mission Partner Environment (MPE), pursuant to the policy and requirements in DoD Instructions (DoDIs) 1000.13 and 8500.01.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION 4
1.1. Applicability. 4
1.2. Policy. 5
1.3. Incorporated and Cancelled Documents. 5
SECTION 2: RESPONSIBILITIES 7
2.1. DoD CIO. 7
2.2. Director, Defense Information Systems Agency (DISA). 8
2.3. Director, DoD PKI PMO. 11
2.4. Under Secretary of Defense for Intelligence and Security. 13
2.5. Director, NSA/Chief, Central Security Service (DIRNSA/CHCSS). 13
2.6. Director, Department of Defense Human Resources Activity 14
2.7. OSD and DoD Component Heads. 15
2.8. Secretary of the Air Force. 16
2.9. Chairman of the Joint Chiefs of Staff. 17
2.10. Commander, United States Cyber Command. 17
SECTION 3: IMPLEMENTING PROCEDURES 18
3.1. PKI. 18
a. DoD Unclassified PKI. 18
b. DoD NSS PKI. 23
c. External PKIs. 27
d. U.S. Coalition PKI. 28
3.2. PKE. 30
a. Authentication. 30
b. Digital Signature. 30
c. Encryption. 32
APPENDIX 3A: CRITERIA FOR ISSUING ALTERNATE TOKENS TO GOS/FOS, SESS, AND THEIR DESIGNATED STAFF 33
3A.1. U.S. GO/FO and SES Staff Credentials and Requirements. 33
3A.2. U.S. GO/FO and SES Credential Requirements. 34
APPENDIX 3B: MISSION PARTNER EXTERNAL PKI APPROVAL PROCESS 35
3B.1. Unclassified Mission Partner and Commercial Vendor External PKI. 35
a. Types of Unclassified Mission Partner and Commercial Vendor External PKIs. 35
b. Unclassified Mission Partner and Commercial Vendor External PKI Approval Criteria. 36
c. Unclassified Mission Partner External PKI Mapping to Approval Criteria. 37
3B.2. Secret Fabric Mission Partner External PKI. 38
a. Federal Executive Branch Department and Agency PKIs. 38
b. DoD-Cleared Contractors Accessing the SIPRNET from Contractor Sites. 38
c. CCEB Partner PKIs. 38
d. Other Mission Partner External PKIs. 39
GLOSSARY 41
G.1. Acronyms. 41
G.2. Definitions. 42

REFERENCES 50

TABLE

Table 1. Mission Partner PKIs on DoD Unclassified Networks 38

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance:

a. Applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this issuance as the "DoD Components").

(2) The Coast Guard, when involving Coast Guard–operated DoD systems and networks and Coast Guard ISs and networks that directly affect the Department of Defense information network and DoD mission assurance, in accordance with the January 19, 2017 Memorandum of Agreement (MOA) between the DoD and Department of Homeland Security.

(3) All DoD unclassified and Secret Fabric networks and ISs under the authority of the Secretary of Defense. Examples include the Non-classified Internet Protocol Router Network (NIPRNET), SECRET Internet Protocol Router Network (SIPRNET), Defense Research and Engineering Network, Secret Defense Research and Engineering Network, SIPRNET Releasable Demilitarized Zone, DoD MPE, and contractor ISs under the National Industrial Security Program. ISs include those that are owned and operated by or on behalf of the DoD, including systems and system components hosted at DoD data centers, contractor-operated systems processing DoD-owned information, and cloud-hosted systems including a platform as a service and infrastructure as a service.

(4) All DoD and non-DoD entities including person entities and non-person entities (NPEs) (e.g., physical devices, virtual machines, ISs, robotic process automation and artificial intelligence bots, other processes) logically accessing unclassified or Secret Fabric networks and ISs under the authority of the Secretary of Defense, including DoD mission partners and DoD beneficiaries.

b. Does not apply to:

(1) IS processing, storing, or transmitting sensitive compartmented information under the existing authorities and policies of the Director of National Intelligence pursuant to Executive Order 12333 and other laws and regulations.

(2) ISs operated by the DoD Special Access Program community. Due to the highly sensitive nature of special access programs and their materials, these systems must be managed independently and fall under the purview of the DoD Special Access Program Chief Information Officer (CIO).

1.2. POLICY.

a. The DoD operates and maintains the DoD unclassified PKI on DoD unclassified networks, the DoD National Security System (NSS) PKI on DoD Secret Fabric networks, and the U.S. Coalition PKI on networks within the DoD MPE as DoD enterprise identity, credential, and access management (ICAM) services.

b. DoD IS owners on the DoD unclassified and Secret Fabric networks, and networks within the MPE, must enable ISs to accept and use DoD-approved PKI certificates:

(1) To digitally sign e-mails and documents.

(2) To support encryption of information in transit (e.g., e-mail, transport layer security).

(3) For smart-card logon to DoD networks in accordance with DoDI 8520.03.

(4) As the principal means of authenticating person and NPEs to DoD systems and applications. See DoDI 8520.03 for circumstances where DoD-approved alternative means of identity authentication are permitted.

(5) To support additional functions that the DoD CIO mandates.

c. The DoD CIO may approve PKIs operated by DoD mission partners and commercial vendors for use by DoD ISs to support e-mail signature and encryption, encryption of information in transit, and authentication to DoD resources.

1.3. INCORPORATED AND CANCELLED DOCUMENTS.

This issuance incorporates and cancels:

a. Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "Department of Defense External Interoperability Plan," August 26, 2010

b. Office of the Chief Information Officer Memorandum, "Approval of External Public Key Infrastructures," July 22, 2008

c. Office of the Chief Information Officer Memorandum, "Combined Communications Electronic Board Interoperability on Secret Networks," July 30, 2012

d. Office of the Chief Information Officer Memorandum, "Commercial Public Key Infrastructure Certificates on Public-Facing DoD Websites," November 8, 2021

e. Office of the Chief Information Officer Memorandum, "Department of Defense Acceptance and Use of Personal Identity Verification-Interoperable (PIV-I) Credentials," October 5, 2010

f. Office of the Chief Information Officer Memorandum, "DoD Guidance on Use of PKI Certificates for Digital Signature," February 3, 2011

g. Office of the Chief Information Officer Memorandum, "DoD Requirements for Accepting NFI Identity Credentials," January 24, 2013

h. Office of the Chief Information Officer Memorandum, "DoD-wide Digital Signature Interoperability," May 5, 2006

i. Office of the Chief Information Officer Memorandum, "Encryption of E-mails between the Department of Defense and its Mission Partners," December 16, 2019

j. Office of the Chief Information Officer Memorandum, "Interim Digital Authentication Guidelines for Unclassified and Secret Classified DoD Networks and Information Systems," August 20, 2018

k. Office of the Chief Information Officer Memorandum, "Issuance of a Second Secret Internet Protocol Router Network Public Key Infrastructure Token to Army Senior Leaders," July 8, 2015

l. Office of the Chief Information Officer Memorandum, "Public Key Infrastructure (PKI) Interoperability with Five Eyes (FVEY) Partner Nations on the Nonsecure Internet Protocol Router Network (NIPRNet)," May 8, 2012

m. Office of the Chief Information Officer Memorandum, "Requirements for Public Key Infrastructure Certificates Non-Person Entities on the Non-classified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network," May 10, 2013

n. Office of the Chief Information Officer Memorandum, "Secret Internet Protocol Router Network Public Key Infrastructure Tokens for Contractor Secret Internet Protocol Router Network Enclaves," July 14, 2017

SECTION 2: RESPONSIBILITIES

2.1. DOD CIO.

In addition to the responsibilities in Paragraph 2.7., the DoD CIO:

a. Oversees the implementation and evolution of the DoD PKI in accordance with DoDIs 1000.13, 1000.25, and 8500.01.

b. Directs, controls, oversees, and provides guidance for all aspects of the DoD PKI Program and changes to the DoD unclassified and NSS PKIs.

c. Develops strategy, establishes priorities, and coordinates responsibilities and requirements for the DoD PKI Program.

d. Serves as the policy management authority (PMA) for the DoD unclassified PKI and the DoD external certification authority (ECA) PKI and approves changes to the DoD unclassified PKI and DoD ECA PKI certificate policies (CPs).

e. Serves as the authorizing official for the DoD PKI Program and approves the Enterprise Authority to Operate for the DoD PKI Program.

f. Approves DoD PKI form factors other than the common access card (CAC) or NSS SIPRNET PKI credential for DoD PKI identity, authentication, signature, device, code signing, group and role, and encryption certificates on unclassified DoD networks (e.g., NIPRNET Enterprise Alternate Token System (NEATS) Alternate Token, mobile PKI solutions or credentials).

g. Approves alternatives to PKI for network logon and system authentication in accordance with DoDI 8520.03.

h. Upon the request of the DoD PKI Program Management Office (PMO), evaluates and approves the release of independent compliance audit letters to Federal or other PKI entities with which the DoD has a relationship.

i. Upon the request of the DoD PKI PMO, assists in notifying DoD Components when new DoD and NSS PKI certification authorities (CAs) are established and in directing DoD Components and system owners to install new CA public certificates in their respective systems and application PKI trust stores.

j. Oversees and facilitates the DoD-approval process for external PKIs by:

(1) Evaluating external PKIs for approval for use on unclassified and secret fabric networks and systems.

(2) Negotiating and signing DoD PKI interoperability MOAs and cross-certification agreements with external PKIs or PKI certificate providers.

k. Ensures the establishment and maintenance of a cross-certification relationship between the DoD unclassified PKI and Federal PKI in accordance with the Federal PKI Policy Authority X.509 CP for the U.S. Federal PKI CP Framework.

l. Collaborates with the Federal PKI community, DoD voting member of the Federal PKI Policy Authority, and Committee on National Security Systems to verify the acceptance of the DoD unclassified PKI, DoD ECA PKI, and DoD NSS PKI by other Federal Executive Branch departments and agencies.

m. Assigns or delegates DoD representation for meetings of government and commercial PKI working groups and organizations such as the CA/Browser forum and the Federal PKI, as necessary.

n. Coordinates implementation of the U.S. Coalition PKI with the DoD Executive Agent (EA) for the DoD MPE.

o. Directs the deployment and use of new PKI-based technologies as they mature and become commercially available upon direction from the National Security Agency (NSA).

p. Collaborates with the PKI PMO on periodic upgrades to the DoD unclassified PKI and the DoD NSS PKI to stronger public key–based cryptographic algorithms (e.g., hashing, encryption, and quantum-resistant algorithms), and associated key sizes and parameters, to meet DoD security and interoperability needs.

q. Directs DoD Components to configure their information technology (IT) to support stronger public key–based cryptographic algorithms (e.g., hashing, encryption, and quantum-resistant algorithms) and associated key sizes and parameters to meet DoD security and interoperability needs pursuant to NSA direction.

r. Provides oversight of the DoD EA for the U.S. Coalition PKI in accordance with the policy and requirements in DoDD 5101.22E.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA).

Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.7., the Director, DISA:

a. In accordance with the April 9, 1999 Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, appoints the Deputy Program Manager of the DoD PKI PMO.

b. Provides PKI operational support to the DoD PKI PMO.

c. Coordinates DISA PKI operational and implementation activities with the Director of the DoD PKI PMO.

d. Takes over operation and sustainment of certain PKI systems and capabilities from the NSA after the transition of the DoD PKI Program.

e. Operates and maintains intermediate CAs, issuing CAs, certificate validation services, and key recovery services for the DoD unclassified PKI, including:

(1) Maintaining a certification practice statement (CPS) for intermediate CAs, issuing CAs, certificate validation services, and key recovery services for the DoD unclassified PKI in accordance with the DoD X.509 CP.

(2) Operating intermediate CAs and issuing CAs, certificate validation services, and key recovery services in accordance with the associated CPS.

(3) Facilitating third-party audits for each system that the DISA runs that support the DoD unclassified PKI and providing results to the DoD PKI PMO and the DoD CIO.

f. Operates and maintains issuing CAs, certificate validation services, and key recovery services for the DoD NSS PKI, including:

(1) Maintaining a CPS for issuing CAs, certificate validation services, and key recovery services for the DoD portion of the NSS PKI in accordance with Committee on National Security Systems Instruction (CNSSI) 1300.

(2) Operating issuing CAs, certificate validation services, and key recovery services in accordance with the associated CPS.

(3) Facilitating third-party audits for each system that the DISA runs that support the DoD NSS PKI and providing results to the DoD PKI PMO.

g. As the common service provider for the NSS PKI, operates and maintains the NSS PKI, to include:

(1) Maintaining a CPS for intermediate CAs, issuing CAs, certificate validation services, and key recovery services in accordance with CNSSI 1300.

(2) Operating and maintaining intermediate CAs, issuing CAs, certificate validation services, and key recovery services in accordance with the associated CPS.

(3) Facilitating third-party audits for each system that the DISA runs that support the NSS PKI common service provider and providing results to the DoD PKI PMO.

h. Coordinates with the Federal PKI to support the development of a Federal public trust PKI, an unclassified NPE PKI, which, it is anticipated, most widely used commercial web browsers and operating systems will trust.

i. Drafts, develops, and maintains PKI-related security technical information guides and security requirements guides.

j. Makes CA services available, including the recovery of private keys associated with encryption certificates, retrieval of archived PKI certificates, and the publication and distribution of certificate revocation information.

k. Designates and maintains a repository for listing DoD-approved external PKIs and posts root and intermediate CA certificates and policy object identifiers (OIDs) of DoD-approved unclassified and Secret Fabric external PKIs, which are updated at least quarterly.

l. Maintains and oversees the ECA Program on behalf of the DoD CIO and appoints the ECA external liaison officer. The ECA external liaison officer:

(1) Acts as the point of contact to receive and coordinate all communications between the ECA community, DoD programs, and DoD PKI PMO.

(2) Publishes their name and contact information on a DoD website accessible to CAC holders.

m. Supports PKE and PKI implementation on DoD networks and systems by:

(1) Designating, maintaining, and regularly updating a DoD repository of policies, best practices, lessons learned, and technical guidance for implementing PKI on DoD IT resources.

(2) Providing PK-enabling support and assistance to DoD Components' PK-enabling help desks.

(3) Providing PK-enabling support and assistance directly to end users, personnel, and system owners within DoD organizations and DoD mission partners who do not have dedicated PK-enabling support.

(4) Advising DoD Components on how to support and accept DoD-approved external PKIs such as DoD-approved mission partner PKIs.

(5) Maintaining, publicizing, and making available to DoD users contact information for DoD-wide and DoD Component PKI and PKE supporting offices (e.g., the DoD PKE team).

(6) Implementing and sustaining the SIPRNET PKI Token Management System and NPE systems on SIPRNET and NIPRNET.

n. Provides a DoD enterprise mobile PKI credentialing capability.

o. Provides cybersecurity services for DISA-operated DoD PKI capabilities in accordance with DoDI 8530.01.

p. Performs the Registration Authority (RA) Audits for both the DoD unclassified and NSS PKIs.

q. Hosts the Global Directory Service, which makes available CA certificates and Certificate Revocation Lists (CRLs) for the DoD, ECA, and NSS PKIs. In addition, the Global Directory

Service provides PKI-authenticated access to public e-mail encryption certificates for DoD and NSS PK-enabled end users.

r. Notifies the DoD CIO when new DoD unclassified PKI and NSS PKI CAs are established.

s. The Joint Interoperability Test Command (JITC) is the designated operational test agency for the DoD PKI Program.

t. The JITC is responsible for operating and maintaining the PKI testing labs in support of the DoD PKI. These responsibilities include, but are not limited to:

(1) Testing support as needed for the operation and sustainment of the DoD PKI.

(2) Providing an environment to support interoperability testing with the Defense Manpower Data Center's (DMDC's) Real-Time Automated Personnel Identification System (RAPIDS) infrastructure for sustainment and technology refresh purposes.

(3) Testing the interoperability of DoD-approved and external PKIs with DoD unclassified and Secret Fabric networks and ISs.

(4) Upon request from DoD Components, testing commercial off-the-shelf products for PKI compatibility.

2.3. DIRECTOR, DOD PKI PMO.

Under the authority, direction, and control of the DoD CIO, and in accordance with the April 9, 1999 Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, the Director, DoD PKI PMO:

a. In coordination with the NSA, DISA, and DMDC, gathers DoD PKI requirements and recommends strategy and priorities for the DoD PKI Program to the DoD CIO.

b. Supports the DoD PKI Program after the formal end of DoD PKI acquisition activities.

c. Coordinates PKI functional requirements from the DoD Components heads and the Federal PKI.

d. Coordinates with the DMDC on changes to DoD unclassified PKI certificate profiles, configuration changes to the CAC, and PKI-related requirements for the CAC RAPIDS.

e. Coordinates with the Under Secretary of Defense for Intelligence and Security to verify that designated DoD unclassified PKI credentials (e.g., the CAC) can properly interface with physical access control systems.

f. Consults with the NSA on the latest threats to and vulnerabilities of the DoD unclassified and NSS PKIs.

g. Coordinates with the Chairman of the Joint Chiefs of Staff, DoD Component heads, the Secretary of the Air Force as the DoD EA for the DoD MPE, the Committee on National Security Systems' PKI member governing body, and the intelligence community PKI manager to verify that the DoD PKI and deployed public key–enabled ISs are capable of supporting joint-, allied-, and coalition-based operations when required.

h. Directs operating feedback mechanisms to identify gaps in DoD PKI capabilities or policies.

i. Facilitates cross-organizational efforts to explore emerging requirements for credentialing for commercial solutions for classified networks and systems.

j. Provides systems engineering and developmental testing for the DoD PKI Program.

k. Requires the DoD unclassified PKI and the DoD NSS PKI to support issuance and requirements for group, role, NPE, code signing, IT privileged user, and general user PKI certificates on DoD unclassified and Secret Fabric networks.

l. Approves the DoD Root CA's issuance and modification of CA certificates.

m. In consultation with the DoD CIO, periodically upgrades the DoD unclassified PKI and the DoD NSS PKI to stronger public key–based cryptographic algorithms (e.g., hashing, encryption, and quantum-resistant algorithms), and associated key sizes and parameters, to meet DoD security and interoperability needs.

n. Collects PKI third-party audit packages for the DoD unclassified PKI and the DoD NSS PKI from the DISA, NSA, and DMDC and provides the packages to the DoD CIO for review and approval for release to the Federal PKI and NSS PKI member governing body.

o. Provides representation to the NSS PKI member governing body to vote and comment on NSS PKI-related documents that the NSS PKI member governing body evaluates.

p. Leads a working group (e.g., the Certificate Policy Management Working Group) to:

(1) Review change proposals for the DoD, ECA, S-Interoperability Domain, and Web Content Filter (WCF) X.509 PKI CPs and make recommendations to their respective PMAs for inclusion of the change proposals.

(2) Review X.509 CPSs for DoD, ECA, S-Interoperability Domain, and WCF Certificate Management Authorities and make recommendations for approval to their respective PMAs.

(3) Review change proposals for the Federal PKI CPs to identify impacts to the DoD or ECA CPs.

(4) Perform comparability analysis of external PKI CPs and CPSs for external PKIs being considered for approval by the DoD CIO.

(5) Review DoD NSS PKI CPSs before their submission to the NSS PKI MGB in accordance with CNSSI 1300.

q. Coordinates with the Secretary of the Air Force, who is the DoD EA for the DoD MPE, on the U.S. Coalition PKI.

2.4. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY.

In addition to the responsibilities in Paragraph 2.7., the Under Secretary of Defense for Intelligence and Security:

a. Coordinates with the PKI PMO to verify that designated DoD unclassified PKI credentials (e.g., the CAC) can properly interface with physical access control systems.

b. Works with the DoD CIO and the DoD PKI PMO to integrate PKI into physical access control systems.

2.5. DIRECTOR, NSA/CHIEF, CENTRAL SECURITY SERVICE (DIRNSA/CHCSS).

Under the authority, direction, and control of the Under Secretary of Defense for Intelligence and Security; the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the NSA, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.7., the DIRNSA/CHCSS, in coordination with the DoD Chief Information Security Officer:

a. Appoints the Director of the DoD PKI PMO in accordance with the April 9, 1999 Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum.

b. Operates and maintains the root CAs for the DoD unclassified PKI, ECA PKI, and NSS PKI and the intermediate CAs for the DoD NSS PKI. They accomplish this by:

(1) Maintaining a CPS for DoD unclassified PKI root CAs in accordance with the DoD X.509 CP.

(2) Maintaining a CPS for NSS PKI root CAs in accordance with Committee on National Security Systems Directive (CNSSD) 506, Committee on National Security Systems Policy (CNSSP) 25, and CNSSI 1300.

(3) Maintaining a CPS for ECA PKI root CAs in accordance with the ECA CP.

(4) Operating the root CAs in accordance with the associated CPS.

(5) Facilitating third-party audits for each root CA and providing results to the DoD PKI PMO.

c. Maintains the design of the DoD NSS PKI commercial credential cardstock in accordance with CNSSD 506, CNSSP 25, and CNSSI 1300 and provides technical support on smart-card technology matters that impact the DoD portion of the NSS PKI.

d. Upon request, provides security reviews to the DoD PKI PMO and the DoD CIO on:

(1) DoD-approved external PKIs and external PKIs being considered for DoD approval.

(2) Changes to PKI operations.

(3) Federal PKI requirements.

(4) Threats to and vulnerabilities of the DoD and NSS PKIs.

e. Deploys new PKI-based authentication and encryption technologies throughout the DoD under the direction and guidance of the DoD CIO as they become available.

f. Supports the DoD PKI PMO.

2.6. DIRECTOR, DEPARTMENT OF DEFENSE HUMAN RESOURCES ACTIVITY.

Under the authority, direction, and control of the Under Secretary of Defense for Personnel and Readiness and in addition to the responsibilities in Paragraph 2.7., the Director, Department of Defense Human Resources Activity, ensures that the Director, DMDC:

a. Maintains the RAPIDS and the Alternate Token Information Management System and supports infrastructure to support the issuance of DoD unclassified PKI certificates on unclassified CACs and other form factors (e.g., NEATS alternate tokens) in coordination with the DoD PKI PMO, to include:

(1) Maintaining a CPS for issuing CACs and operating the NIPRNET credential issuance infrastructure in accordance with the DoD X.509 CP.

(2) Operating the CAC RAPIDS and the NIPRNET-credential issuance infrastructure systems in accordance with the applicable CPS.

(3) Facilitating third-party audits for the CAC RAPIDS, the Alternate Token Information Management System, and the NIPRNET credential issuance infrastructure against the applicable CPS and providing results to the DoD PKI PMO.

(4) Implementing and sustaining the NEATS to provide enterprise alternate credentials.

(5) Provides Tier 1, 2, and 3 help desk support and assistance to provisioned operators of the Alternate Token Information Management System and the NEATS.

b. Maintains the CAC design in accordance with National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) Publication 201-2 and the

Federal PKI common policy and provides technical support to the DoD PKI PMO on smart-card technology matters that impact the DoD unclassified and NSS PKIs.

c. Coordinates with the DoD PKI PMO and DoD Identity Protection and Management Senior Coordinating Group on requirements and configuration changes to the CAC and other DoD PKI smart-card credentials and changes to DoD unclassified PKI certificate profiles.

d. Provides cybersecurity services for DMDC-operated DoD PKI capabilities in accordance with DoDI 8530.01.

2.7. OSD AND DOD COMPONENT HEADS.

The OSD and DoD Component heads:

a. Support the DoD unclassified, NSS, and U.S. Coalition PKI certificate life cycles from issuance to cancellation and key recovery for both person entities and NPEs by:

(1) Appointing and managing RAs and local registration authorities (LRAs) as specified in the DoD RA and LRA CPSs and DoD registration practice statements.

(2) Submitting addendums to the DoD PKI PMO for approval of DoD Component–specific variations to the DoD RA and LRA CPS to verify compliance with the DoD X.509 CP for issuing DoD unclassified PKI certificates and the DoD registration practice statement to verify compliance with CNSSI 1300 for issuing DoD NSS PKI certificates.

(3) Providing trained personnel to perform RA and LRA activities that conform to the associated CPS or registration practice statement.

(4) Facilitating compliance audits of RA and LRA operations as specified in the approved practice statements and providing results to the DoD PKI PMO.

(5) Providing trained personnel to perform Purebred agent/supervised mobile credentialing enrollment support.

b. Manage and oversee the deployment and installation of PKI certificates to NPEs.

c. Rely on DoD-approved PKI certificates when using or accepting PKI for authentication, digital signature, and encryption.

d. Oversee the PK enabling of network accounts, ISs, e-mail systems, web servers, and devices, to include mobile devices, for which the DoD Component is the owner, program executive, lead agency, PMO, or equivalent to process, accept, and use PKI certificates:

(1) To digitally sign e-mails and documents.

(2) To have the ability to encrypt information in transit, as appropriate (e.g., controlled unclassified information).

(3) For authentication to DoD networks in accordance with DoDI 8520.03.

(4) As the principal means of authenticating persons and NPEs. See DoDI 8520.03 for DoD-approved alternative means of identity authentication.

e. Coordinate with the DoD PKI PMO on functional requirements supporting the DoD PKI upgrade and maintenance process.

f. Coordinate with the Secretary of the Air Force, who is the DoD EA for the DoD MPE, on the U.S. Coalition PKI.

g. Coordinate with the DISA to verify that new commercial off-the-shelf software procurements are compatible with DoD-approved PKI.

h. Install and use new PKI-based technologies as the DoD PKI PMO makes them available.

i. Coordinate with the Office of the Chairman of the Joint Chiefs of Staff and the DoD PKI PMO to verify that deployed DoD ISs that are PK-enabled can support joint- and allied-based operations involving users with DoD-approved PKI.

j. Verify that DoD networks, ISs, applications, and devices that are PK-enabled are configured to support the latest public key–based cryptographic algorithms (e.g., hashing, encryption, and quantum-resistant algorithms) and associated key sizes and parameters that the DoD CIO mandates.

k. Direct all DoD contracts to require DoD mission partners who own and operate DoD-approved PKIs to ensure that these PKIs support the latest public key–based cryptographic algorithms that the DoD CIO mandates when interacting with DoD unclassified and Secret Fabric networks and IS and networks within the DoD MPE.

2.8. SECRETARY OF THE AIR FORCE.

In accordance with DoDD 5101.22E and DoDI 8110.01, in addition to the responsibilities in Paragraph 2.7., and in their capacity as the DoD EA for DoD MPE, the Secretary of the Air Force:

a. Operates and maintains the root CAs for the U.S. Coalition PKI and the subordinate CAs where needed for enterprise services. They accomplish this by:

(1) Maintaining a CPS for U.S. Coalition PKI root CAs in accordance with the U.S. Coalition X.509 CP.

(2) Operating the root CAs in accordance with the associated CPSs.

b. Coordinates with DoD Components on the U.S. Coalition PKI.

c. Coordinates with the DoD PKI PMO on the U.S. Coalition PKI.

2.9. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In addition to the responsibilities in Paragraph 2.7., the Chairman of the Joint Chiefs of Staff:

a. Identifies, reviews, and validates public key–enabling requirements for the Combatant Commands and ensures that the Combatant Commanders coordinate requirements to implement this issuance.

b. Coordinates with the DoD PKI PMO, the Secretary of the Air Force as the DoD EA for the DoD MPE, and the DoD Components to verify that deployed PKE ISs are capable of supporting joint-, allied-, and coalition-based operations.

2.10. COMMANDER, UNITED STATES CYBER COMMAND.

In addition to the responsibilities in Paragraph 2.7., the Commander, United States Cyber Command:

a. Monitors ECA PKIs for certificate compromises.

b. Monitors for the misuse of DoD PKI and DoD NSS PKI certificates.

c. Once a Federal public trust PKI is fully operational:

(1) Maintains a log of Federal public trust PKI certificates distributed to DoD ISs.

(2) Monitors commercial certificate transparency logs so as to identify and flag any unauthorized transport layer security certificates issued to the .mil domain and to direct their immediate revocation.

SECTION 3: IMPLEMENTING PROCEDURES

3.1. PKI.

PKIs operating under the purview of the DoD (e.g., DoD unclassified PKI, DoD ECA PKI, U.S. Coalition PKI, DoD NSS PKI) are approved for use for their intended purpose and environment.

a. DoD Unclassified PKI.

(1) PKI Operations.

The DISA, as part of the DoD PKI PMO, must operate the DoD unclassified PKI to satisfy operational needs and requirements on the NIPRNET and other unclassified networks. The DoD unclassified PKI must make its public keys available to DoD mission partners who have access to unclassified DoD networks.

(a) Certificate Issuance.

The DoD unclassified PKI issues certificates to all subscribers identified in the DoD X.509 CP to support DoD missions and business operations. The DoD unclassified PKI may issue different types of PKI certificates to satisfy DoD Component requirements, including identity, authentication, signature, encryption, group and role, device, and code signing.

(b) Certificate Validation.

The DoD unclassified PKI provides certificate revocation data through CRL publication and the robust certificate validation service. The robust certificate validation service is the DoD PKI's Online Certificate Status Protocol responder infrastructure.

(c) Key Recovery.

The DoD unclassified PKI supports first- and third-party key recovery for private keys associated with DoD PKI encryption certificates on DoD unclassified networks.

(2) Hardware Credentials.

All PKI hardware credentials used to access DoD unclassified resources must comply with the requirements of their respective CPs and meet the requirements for Authenticator Assurance Level (AAL) 3.

(a) CACs.

In accordance with Homeland Security Presidential Directive-12 and NIST FIPS Publication 201-2, the personal identity verification (PIV) credential is the primary PKI hardware credential for identifying and authenticating Federal employees and contractors to Federal facilities and unclassified Federal networks and systems. In accordance with DoDI 1000.13, the CAC is the DoD PIV and the primary PKI hardware credential for identifying and authenticating DoD employees and DoD contractors who have been provisioned DoD

network accounts on the NIPRNET and other unclassified DoD network resources. The CAC protects the private keys associated with authentication, signature, and encryption certificates that the DoD PKI issues for use in unclassified environments. DoD personnel and ISs may rely on PKI certificates issued and maintained on the CAC.

(b) Alternate Tokens.

Alternate tokens, which the NEATS issues, are a type of DoD hardware PKI credential for unclassified networks and systems that do not conform to all Federal requirements for PIV. Alternate tokens must not be used as broad replacements for the CAC. Alternate tokens are authorized for specific situations where CACs are not used due to technical or policy reasons. These situations include, but are not limited to:

1. IT privileged user accounts. IT privileged users must use alternate tokens to authenticate to their privileged user accounts.

a. Pursuant to Technical Attachment 1 to United States Cyber Command Tasking Order 14-0018, IT privileged users with domain and enterprise administrator accounts that require smart-card logon must use a different alternate token for these accounts than the alternate token they use to access system administrator accounts. DoD Components may issue multiple alternate tokens to a single IT privileged user for this purpose.

b. If the resource (e.g., device, system) in question cannot support authentication with PKI technology, the IT privileged users must follow procedures in accordance with DoDI 8520.03.

2. Role or watch officer accounts. DoD organizations may issue alternate tokens to individuals who require access to role or watch officer accounts as part of their duties. The organizations must have sign-in and sign-out procedures for the individuals when they report to their position. Only one individual may have and use the alternate token at a time. Under no circumstances may multiple individuals have, access, or use a role or watch officer alternate token simultaneously.

3. U.S. general officer/flag officer (GO/FO), senior executive service (SES), and GO/FO and SES staff accounts. Issuance of alternate tokens to authorized U.S. GO/FO or SES personnel or their staffs must be in accordance with the implementing procedures and restrictions in Appendix 3A.

(c) Hardware Security Module.

The DoD may issue unclassified PKI hardware certificates to hardware security modules that are validated as meeting the requirements of Level 2 or above in NIST FIPS Publication 140-3.

(d) Other Form Factors.

The DoD CIO may approve unclassified PKI hardware credentials other than the CAC or alternate token to facilitate DoD missions on a case-by-case basis.

(3) Software Certificates.

All unclassified PKI software certificates used to access DoD unclassified resources must comply with the requirements of their respective CPs.

(a) Software Certificates for NPEs.

PKI software certificates are primarily intended for identifying and authenticating NPEs such as servers, systems, or other network components or devices. All DoD web servers require a DoD-approved NPE PKI certificate to initiate transport layer security server authentication, support data integrity, and maintain confidentiality.

(b) Software Certificates for Person Entities.

DoDI 8520.03 outlines the specific use cases, situations, and requirements where users may authenticate to DoD IT resources with PKI software certificates. DoD PKI software certificates may not be issued to Combined Communications-Electronics Board (CCEB) users to support authentication to unclassified DoD networks.

(c) Mobile PKI Solutions.

The Purebred mobile PKI solution is currently the only DoD-approved capability for deploying DoD unclassified mobile PKI credentials to DoD unclassified mobile endpoints. The DoD CIO may approve other mobile PKI solutions and credentials under separate guidance. DoD mobile PKI credentials will:

1. Be issued only to requesters possessing a valid DoD PKI hardware credential (e.g., the CAC, alternate token). Requestor verification must be performed through a PKI authentication.

2. Identify the possessor by asserting the same common name as the DoD PKI certificate on the DoD PKI hardware credential.

3. Be issued, used, stored, and managed in accordance with the December 20, 2019 DoD CIO Memorandum.

(4) NPE Certificates.

DoD Components and their system owners must install NPE PKI certificates on all unclassified DoD Internet Protocol–enabled devices (e.g., web servers, network devices such as domain controllers and routers, mobile phones, Internet of Things devices) to support authentication. NPE certificates may also be issued to robotic process automation, artificial intelligence, or other NPEs that perform actions on behalf of individuals or organizations.

Depending on the specific use case, NPE PKI certificates will be issued to unclassified DoD NPEs from one of these PKIs:

(a) DoD Unclassified PKI.

NPE certificates that the DoD unclassified PKI issues must be installed on unclassified systems or devices regularly accessed by users from other DoD Components or mission partners but that are not public facing. NPE PKI certificates that the DoD unclassified PKI issues must align with one of the CP OIDs in the DoD Unclassified PKI CP. PKI certificates issued through the DoD PKI NPE Portal may not be used as user certificates.

(b) Only Locally Trusted (OLT) Unclassified PKI.

Some DoD Components own and operate their own internal unclassified PKIs, termed "OLT PKIs" for purposes of this policy, for use on unclassified DoD networks and systems. These OLT PKIs do not align with the CP OIDs in the DoD unclassified PKI CP and are not authorized to issue PKI certificates or credentials to personnel. These DoD Component OLT PKIs are approved to issue NPE PKI certificates to unclassified DoD NPEs provided that:

1. The certificate is issued to a system or device.

2. Certificate use is bound to the individual local DoD Component network where the OLT PKI and the NPE are located. Relying parties from other DoD Components do not regularly access the system or device.

3. The unauthorized disclosure (i.e., loss of confidentiality) or modification (i.e., loss of integrity) of information sent to or from the system or device will not have a high-impact potential pursuant to NIST FIPS Publication 199.

(c) Commercial Unclassified PKI.

DoD Components and system owners may install transport layer security 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 all the conditions in Paragraphs 3.1.a.(4)(c)1.-5. are met:

1. The DoD website or EEMSG mail server must be 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 IS network, then it must be hosted in an appropriately isolated network segment (e.g., a DoD demilitarized 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 uses the Secure Hash Algorithm-256 or a stronger hash algorithm and is issued under a Secure Hash Algorithm-256 or stronger root CA.

5. The commercial NPE PKI certificate is 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/.

(d) Unclassified Federal Public Trust PKI.

DoD is working with the General Services Administration (GSA)-run Federal PKI to develop a Federal public trust PKI, which, it is anticipated, most widely used commercial web browsers, operating systems, and mail servers will trust. Once a Federal public trust PKI is fully operational, DoD Components using commercial PKI certificates in accordance with Paragraph 3.1.a.(4)(c) must transition to certificates that the Federal public trust PKI issues, as the previously obtained commercial PKI certificates expire.

(5) Code-Signing Certificates.

DoD Components and system owners may certify code on their websites with PKI code-signing certificates. Depending on the specific use case, DoD Components and system owners may use code-signing certificates from the PKIs listed in Paragraph 3.a.(5)(a)-(b) to certify code on their unclassified DoD websites:

(a) Commercial PKI.

DoD Components and system owners may use code-signing PKI certificates that a commercial PKI issues to certify code on their unclassified DoD websites, provided that the conditions in Paragraphs 3.1.a.(5)(a)1.-5. are met:

1. The DoD website is public facing.

2. If the DoD website is hosted on a defense IS network, then it must be hosted in an appropriately isolated network segment (e.g., a DoD demilitarized 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 PKI certificate uses the Secure Hash Algorithm-256 or a stronger hash algorithm and is issued under a Secure Hash Algorithm-256 or stronger root CA.

5. The commercial PKI certificate is 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/.

(b) DoD Unclassified PKI.

All code-signing PKI certificates on unclassified DoD websites that do not meet the criteria in Paragraph 3.1.a.(4)(c) for commercial issuance must be issued by the DoD unclassified PKI.

(6) Trusted Platform Modules.

PKI certificates that meet the requirements for AAL 2 (i.e., software PKI) may be issued to unclassified devices (e.g., workstations) leveraging trusted platform modules that have been validated at NIST FIPS Publication 140-3 Security Level 1 or above. PKI certificates that meet the requirements for AAL 3 (i.e., hardware PKI) may be issued to unclassified devices (e.g., workstations) leveraging trusted platform modules validated at NIST FIPS Publication 140-3 Security Level 2 or above.

(7) WCF PKI.

CAs used to facilitate WCF at a DoD unclassified network boundary must be operated in accordance with the WCF X.509 CP.

b. DoD NSS PKI.

(1) PKI Operations.

The DISA, as part of the DoD PKI PMO, implements the DoD NSS PKI to satisfy operational needs and requirements on the SIPRNET and other DoD Secret Fabric networks. The DoD NSS PKI must make its public keys available to DoD mission partners who have been granted access to DoD Secret Fabric networks.

(a) Certificate Issuance.

The DoD NSS PKI issues certificates to designated subscribers in accordance with CNSSD 506, CNSSP 25, and CNSSI 1300 to support DoD missions. The DoD NSS PKI may issue different types of PKI certificates to satisfy DoD Component requirements, including identity, authentication, signature, encryption, group and role, device, and code-signing certificates.

(b) Certificate Revocation.

The DoD NSS PKI provides certificate revocation data through the CRL publication and the robust certificate validation service.

(c) Key Recovery.

The DoD NSS PKI supports first- and third-party key recovery for private keys associated with DoD PKI encryption certificates on DoD Secret Fabric networks. Robust certificate validation service is the DoD NSS PKI's Online Certificate Status Protocol responder infrastructure.

(2) Hardware Certificates.

All PKI hardware credentials used to access DoD Secret Fabric resources must comply with their respective CPs. The DoD NSS PKI hardware credentials protect the private keys associated with identity, authentication, signature, and encryption certificates that the DoD NSS PKI issues for use in secret fabric environments in accordance with CNSSD 506, CNSSP 25, and CNSSI 1300. DoD NSS PKI hardware credentials may be issued as:

(a) Individual Subscriber Credentials.

1. In accordance with CNSSP 25, the NSS PKI hardware credential is the primary PKI hardware credential for authenticating U.S. Government Department and Agency employees and contractors to Federal Secret Fabric networks and systems. The DoD NSS PKI hardware credential is the primary PKI hardware credential for authenticating DoD employees and DoD contractors who have been provisioned DoD network accounts on the SIPRNET and other DoD Secret Fabric network resources. These credentials fulfill similar functions on the DoD Secret Fabric networks as CACs on unclassified DoD networks in that they contain PKI certificates to facilitate authentication, digital signature, and e-mail encryption.

2. DoD personnel and relying parties can rely on PKI certificates issued and maintained on the DoD NSS PKI hardware credential. All DoD NSS PKI credentials issued at assurance levels appropriate for a given system and user community are approved for acceptance by DoD-relying parties, be they issued by DoD or other Federal Executive Branch departments or agencies.

(b) Credentials for CCEB Foreign Nationals in the Defense Personnel Exchange Program.

1. DoD Components may issue DoD NSS PKI hardware credentials to CCEB foreign nationals hosted under the Defense Personnel Exchange Program for purposes of authenticating to CCEB-releasable DoD Secret Fabric resources. When facilitating access for these CCEB foreign nationals to CCEB-releasable DoD Secret Fabric resources, DoD Components must comply with the access and implementation requirements for foreign nationals in DoDDs 5230.11 and 5230.20; DoDIs 5530.03 and 8500.01; and applicable DISA security technical information guides (e.g., the DISA Releasable Embedded Local Area Network Security Technical Information Guide Overview).

2. DoD Components must not issue DoD NSS PKI credentials to CCEB foreign nationals who are:

a. Foreign liaison officers.

b. Cooperative program personnel.

(c) Special-Purpose DoD NSS PKI Credentials.

DoD NSS PKI hardware credentials can be configured for special purposes similar to what alternate tokens are used for on unclassified DoD networks. These special purposes include, but are not limited to:

1. IT privileged user accounts. Admin-I credentials are DoD NSS PKI hardware credentials used by IT privileged users who have only a PKI authentication certificate. They are used for authentication to DoD Secret Fabric IT privileged user accounts.

2. Role or watch officer accounts. DoD organizations may issue special-purpose DoD NSS PKI credentials to individuals who require access to role or watch officer accounts as part of their duties. The organizations must have sign-in and sign-out procedures for the individuals when they report to their position. Only one individual may have and use the special-purpose DoD NSS PKI credential at a time. Under no circumstances may multiple individuals have, access, or use a role or watch officer special-purpose DoD NSS PKI credential simultaneously.

3. U.S. GO/FO, SES, and GO/FO and SES staff accounts. Issuance of special-purpose DoD NSS PKI credentials to authorized U.S. GO/FO or SES personnel or their staffs must be in accordance with the implementing procedures and restrictions in Appendix 3A.

(3) Software Certificates.

All PKI software certificates used to access DoD Secret Fabric resources must comply with the requirements of their respective CPs.

(a) Software Certificates for NPEs.

PKI software certificates are primarily intended for identifying and authenticating NPEs such as servers, systems, or other network components or devices. All DoD Secret Fabric web servers require a DoD-approved NPE PKI certificate to initiate transport layer security server authentication, support data integrity, and maintain confidentiality.

(b) Software Certificates for Person Entities.

DoDI 8520.03 outlines the specific use cases, situations, and requirements where users may authenticate to DoD IT resources with PKI software certificates.

(c) Mobile PKI Solutions.

PKI credentials for DoD Secret Fabric mobile endpoints must use National Information Assurance Partnership–approved solutions.

(4) NPE Certificates.

DoD Components and their system owners must install NPE PKI certificates on all DoD Secret Fabric Internet Protocol–enabled devices (e.g., web servers, network devices such as domain controllers and routers, mobile phones, Internet of Things devices) to support

authentication. NPE certificates may also be issued to robotic process automation, artificial intelligence, or other NPEs that perform actions on behalf of individuals or organizations. Depending on the specific use case, NPE PKI certificates will be issued to DoD Secret Fabric NPEs from one of these PKIs:

(a) DoD NSS PKI.

DoD Components and systems owners must install NPE PKI certificates issued by the DoD NSS PKI on DoD Secret Fabric systems or devices regularly accessed by users from other DoD Components or outside the DoD.

(b) OLT PKI.

Some DoD Components own and operate their OLT PKIs for use on DoD Secret Fabric networks and systems. These OLT PKIs do not align to the CP OIDs in the NSS PKI CP and are not authorized to issue PKI certificates or credentials to personnel. These DoD Component OLT PKIs are approved to issue NPE PKI certificates to DoD Secret Fabric systems or devices provided that:

1. The OLT PKI meets all the requirements for a DoD Secret Fabric OLT PKI in CNSSD 506.

2. The certificates are issued only to system or device subscribers pursuant to CNSSI 1300.

3. Certificate use is bound to the individual local DoD Component network where the NPE OLT CA and the NPE are located.

(c) PMA-Approved PKI.

Per CNSSD 506, the NSS PKI PMA may authorize the operation of department or agency internal Secret Fabric PKIs that are not part of the NSS PKI and do not meet the guidelines for an NPE OLT PKI. Per CNSSI 1300, the PMA for the NSS PKI is the DIRNSA/CHCSS.

(5) Code-Signing Certificates.

DoD Components and system owners may certify code on their Secret Fabric websites with PKI code-signing certificates. On DoD Secret Fabric websites and resources, DoD Components and system owners may use only code-signing certificates issued by the DoD NSS PKI to certify code.

(6) Trusted Platform Modules.

DoD NSS PKI certificates that meet the requirements for AAL 2 (i.e., software PKI) may be issued to devices (e.g., workstations) leveraging trusted platform modules validated at NIST FIPS Publication 140-3 Security Level 1 or above. DoD NSS PKI certificates that meet the requirements for AAL 3 (i.e., hardware PKI) may be issued to devices (e.g., workstations)

leveraging trusted platform modules validated at NIST FIPS Publication 140-3 Security Level 2 or above.

(7) WCF PKI.

CAs used to facilitate web content filtering at a DoD Secret Fabric network boundary must be operated in accordance with the WCF X.509 CP.

c. External PKIs.

External PKIs are non-DoD PKIs that provide PKI certificates to DoD mission partners. External PKIs include ECAs and PKIs that mission partners or commercial vendors operate. DoD ISs may rely only on external PKIs that the DoD CIO approves. The DoD-approval process for mission partner PKIs can be found in Appendix 3B. DoD-approved external PKI user certificates can be used for authenticating to DoD websites and applications, digitally signing e-mails and documents, and encrypting e-mails. DISA maintains a repository for DoD-approved external PKIs at https://cyber.mil/pki-pke/interoperability. Questions about the DoD external PKI approval process should be submitted to osd.mc-alex.dod-cio.mbx.icam@mail.mil.

(1) ECA.

The DoD must maintain the DoD unclassified ECA PKI Program in accordance with the ECA X.509 CP to support certificate issuance to DoD mission partners, including CCEB partners and other foreign partners on foreign soil for use on DoD unclassified networks such as the NIPRNET. CCEB partners may be issued ECA certificates only at medium token assurance or above. The ECA PKI Program must make its public keys available to DoD mission partners on unclassified networks. ECAs may be used only on unclassified networks and not on classified networks. For more information, see the ECA X.509 CP, which requires:

(a) The NSA to operate the ECA root CA.

(b) The DISA to maintain a repository for DoD ECA information. The current repository is at https://cyber.mil/eca/.

(c) Issuance of DoD ECA PKI certificates in accordance with the DoD ECA X.509 CP to be approved for use on DoD unclassified networks at the appropriate level of assurance. The ECA levels of assurance are medium, medium token, and medium hardware. ECA medium assurance certificates are software PKI certificates and should be used only as encryption or NPE certificates. ECA medium token and medium hardware assurance PKI certificates are hardware-based PKI credentials intended for person entities. Identity-proofing requirements for ECA medium token assurance and medium hardware assurance PKI credentials vary based on the requester's location:

1. Within the United States, identity proofing for ECA medium token credentials must be done in person with a notary, a third-party trusted agent (TA) of the ECA vendor, or the ECA vendor themselves. Identity proofing for ECA medium hardware credentials must be done

in person with a third-party TA of the ECA vendor or the ECA vendor themselves and cannot be done with a notary.

2. Outside the United States identity proofing for both ECA medium token assurance and medium hardware assurance credentials must be done in person with an authorized DoD employee. The ECA external liaison officer maintains the list of authorized DoD employees. Individuals needing an authorized DoD employee must coordinate with the ECA external liaison officer, who will assist in locating an authorized DoD employee in the specified country.

(2) Mission Partner or Commercial Vendor PKIs.

Mission partner and commercial vendor PKIs are operated externally to the DoD and issue PKI certificates to DoD mission partner users. The DoD CIO will oversee and facilitate the approval of these PKIs as described in Appendix 3B.

(3) Validating External PKIs.

DoD-relying parties must accept DoD-approved external hardware PKI credentials from DoD mission partners with a legitimate need to access DoD information on their systems. DoD-relying parties must validate that PKI certificates issued by DoD-approved external PKIs are using a cross-certification mechanism or a direct trust mechanism. DoD-relying parties can facilitate direct trust for most DoD-approved external PKIs by downloading the PKI trust chains associated with the external PKI from the previously mentioned repository. DoD-relying parties must check the revocation status of PKI certificates issued by DoD-approved external PKIs before accepting them.

d. U.S. Coalition PKI.

(1) PKI Operations.

The DoD EA for MPE implements the U.S. Coalition PKI to satisfy operational needs and requirements on MPE networks. The U.S. Coalition PKI must make its public keys available to DoD mission partners who have been granted access to DoD MPE networks. The DoD EA for MPE will periodically upgrade the U.S. Coalition PKI to stronger public key–based cryptographic algorithms (e.g., hashing, encryption, and quantum-resistant algorithms) and associated key sizes and parameters to meet DoD security and interoperability needs.

(a) Certificate Issuance.

The U.S. Coalition PKI issues certificates to designated subscribers in accordance with the U.S. Coalition X.509 CP to support DoD missions. The U.S. Coalition PKI may issue different types of PKI certificates to satisfy DoD Component requirements, including identity, authentication, signature, encryption, group and role, device, and code-signing certificates.

(b) Certificate Restrictions.

The U.S. Coalition PKI may be used only to authenticate to and access networks within the DoD MPE. The U.S. Coalition PKI is not a part of the DoD PKI and may not be used to authenticate or gain access to the NIPRNET, SIPRNET, Defense Research and Engineering Network, Secret Defense Research and Engineering Network, or any other DoD networks, systems, or information outside the MPE.

(c) Certificate Revocation.

The U.S. Coalition PKI provides certificate revocation data through the CRL publication and the robust certificate validation service.

(d) Key Recovery.

The U.S. Coalition PKI supports key recovery for private keys associated with U.S. Coalition PKI encryption certificates on networks within the DoD MPE.

(e) Special-Purpose U.S. Coalition PKI Credentials.

U.S. Coalition PKI credentials can be configured for special purposes. These special purposes include, but are not limited to:

1. IT privileged user accounts. Administrator credentials are U.S. Coalition PKI hardware credentials used by IT privileged users that only have a PKI authentication certificate. They are used for authentication to DoD MPE IT privileged user accounts.

2. Role or watch officer accounts. DoD organizations may issue special-purpose U.S. Coalition PKI credentials to individuals who require access to role or watch officer accounts as part of their duties. The organizations must have sign-in and sign-out procedures for the individuals when they report to their position. Only one individual may have and use the special-purpose U.S. Coalition PKI credential at a time. Under no circumstances may multiple individuals have, access, or use a role or watch officer special-purpose U.S. Coalition PKI credential simultaneously.

(2) Software Certificates.

All PKI software certificates used to access DoD MPE resources must comply with the requirements of their respective CPs.

(a) Software Certificates for NPEs.

PKI software certificates are intended primarily for identifying and authenticating NPEs such as servers, systems, or other network components or devices. All DoD MPE web servers require a DoD-approved NPE PKI certificate to initiate transport layer security server authentication, support data integrity, and maintain confidentiality.

(b) Software Certificates for Person Entities.

DoDI 8520.03 outlines the specific use cases, situations, and requirements where users may authenticate to DoD IT resources with PKI software certificates.

(3) NPE Certificates.

DoD Components and system owners must install NPE PKI certificates on all DoD MPE Internet Protocol–enabled devices (e.g., web servers, network devices such as domain controllers and routers, mobile phones, Internet of Things devices) to support authentication. NPE certificates may also be issued to robotic process automation, artificial intelligence, or other NPEs that perform actions on behalf of individuals or organizations.

(4) Code-Signing Certificates.

DoD Components and system owners may certify code on their DoD MPE websites with PKI code-signing certificates. On DoD MPE websites and resources, DoD Components and system owners may only use code-signing certificates issued by the U.S. Coalition PKI.

(5) Trusted Platform Modules.

U.S. Coalition PKI certificates that meet the requirements for AAL 2 (i.e., software PKI) may be issued to devices (e.g., workstations) leveraging trusted platform modules validated at NIST FIPS Publication 140-3 Security Level 1 or above.

3.2. PKE.

a. Authentication.

DoDI 8520.03 establishes and implements policy and prescribes procedures for using DoD-approved PKI and other approved technologies to authenticate to DoD networks and ISs to access DoD resources. For more information on PKE, see https://cyber.mil/pki-pke/.

b. Digital Signature.

Disclosure of information contained in DoD PKI certificates to third parties is necessary to support validation of DoD PKI-based digital signatures of e-mails and documents. Accordingly, the disclosure of information contained in DoD PKI certificates, including the signer's name, e-mail address, and DoD-issued Electronic Data Interchange Personal Identifier, is not a breach of personally identifiable information in accordance with DoDI 1000.30 and Volume 2 of DoD Manual 5400.11. PKI certificates may help create a digital signature to support multiple purposes, including, but not limited to:

(1) Document Signature.

In accordance with the January 25, 2013 GSA and Federal CIOs Council guidance, electronic signatures are the equivalent of handwritten signatures and encompass all the methods and technologies by which one can sign an electronic record. All electronic signatures used for

DoD systems, business, or transactions must comply with the electronic signature requirements in Office of Management and Budget Circular A-130 and the January 25, 2013 GSA and Federal CIOs Council guidance. Digital signatures are a subset of electronic signatures that use public key cryptography. PKI allows for implementing digital signatures and can be an important enabling tool to comply with Federal laws. When implemented correctly, digital signatures demonstrate superior integrity, source authentication, and non-repudiation over other forms of electronic signature.

(a) Assessment.

DoD Components and system owners must review and assess whether incorporating a digital signature capability would improve the information security, efficiency, or effectiveness of their processes or transactions.

(b) Requirements.

When digital signatures are used for DoD systems, business, or transactions, they must:

1. Be generated using DoD-approved PKI certificates.

2. Comply with the electronic signature requirements in Office of Management and Budget Circular A-130 and the January 25, 2013 GSA and Federal CIOs Council guidance.

(c) Agreements with Commercial Vendors.

The DoD CIO may establish agreements with commercial vendors to trust and accept DoD unclassified PKI certificates in the commercial vendors' digital signature products and services.

(2) E-Mail Signature.

PKI credentials are used to digitally sign e-mails so that e-mail recipients can confirm that the e-mails were not altered in transit (i.e., data integrity), reliably authenticate the sender, and support technical non-repudiation.

(a) E-mail Digital Signature Procedures.

DoD Components must develop and maintain e-mail digital signature procedures to help facilitate and implement DoD digital signature e-mail requirements.

(b) Capability.

DoD Components must configure their DoD e-mail systems and applications on DoD unclassified and Secret Fabric networks to be able to send and receive digitally signed e-mails. DoD e-mail systems and applications must not invalidate digital signatures using DoD-approved external PKIs with e-mail filters or any other functions. E-mail content protections must not cause e-mail signatures to become invalid for e-mails from internal or external senders.

(c) Default Settings.

The default settings on all workstations must be configured to digitally sign outgoing e-mails but permit users the flexibility to send unsigned e-mails on a case-by-case basis.

(d) User Actions.

DoD users must digitally sign DoD e-mails with their DoD-approved PKI credentials if the e-mails contain:

1. Attachments, embedded hyperlinks, or website addresses.

2. Highly sensitive information such as controlled unclassified information.

3. Official DoD business such as memorandums; travel orders; or contractual, budget, program financial, or proprietary information.

4. Other information requiring data integrity, message source authenticity, or non-repudiation.

c. Encryption.

PKI certificates may be used to support the encryption of data for multiple purposes, including, but not limited to, e-mail encryption. Encrypting e-mails with PKI provides users with the confidence that the e-mails they send and receive have not been read by a third party in transit (i.e., confidentiality). DoD Components must each develop and maintain e-mail encryption procedures to help facilitate and implement DoD encryption requirements for e-mail.

(1) Capability.

All DoD e-mail systems on DoD unclassified and Secret Fabric networks, including those on mobile devices, must support sending and receiving e-mails encrypted using DoD-approved PKI certificates. Medium assurance software PKI certificates issued by DoD-approved PKIs may be used and accepted for purposes of e-mail encryption, but not for digital signatures. See DoDI 8520.03 for identity authentication requirements.

(2) User Actions.

DoD users must:

(a) Whenever technically feasible, encrypt e-mails and attachments that contain controlled unclassified information on unclassified DoD networks. See DoDI 5200.48 for more information on controlled unclassified information.

(b) Use only DoD-approved PKI user certificates to encrypt e-mails and e-mail attachments. For purposes of e-mail encryption, these user certificates may be medium assurance software certificates issued by DoD-approved PKIs.

APPENDIX 3A: CRITERIA FOR ISSUING ALTERNATE TOKENS TO GOS/FOS, SESS, AND THEIR DESIGNATED STAFF

3A.1. U.S. GO/FO AND SES STAFF CREDENTIALS AND REQUIREMENTS.

a. The DoD or OSD Component head must designate, in writing, an approving authority for issuing staff support alternate tokens, special-purpose NSS PKI credentials, or mobile device PKI credentials to U.S. GO/FO and SES designated staff.

b. Participating U.S. GOs/FOs or SESs must designate their individual network account as a group account.

c. One member of the U.S. GO/FO or SES staff must be named, in writing, as the sponsor for the group account. That individual will:

(1) Control and designate which personnel are assigned to the group account.

(2) Request one or more staff support alternate tokens, special-purpose NSS PKI credentials, or mobile PKI credentials from the supporting service's RA. The number of staff support alternate tokens, special-purpose NSS PKI credentials, or mobile device PKI credentials requested will be limited to the minimum needed.

(3) Control and monitor distribution of all authorized and assigned credentials.

d. The local network domain administrator must change the account from an individual to a group account and provide the value of GO/FO or SES user principal name field to the RA or TA providing the alternate tokens, special-purpose NSS PKI credentials, or mobile PKI credentials.

e. The staff support alternate tokens, special-purpose NSS PKI credentials, and mobile PKI credentials will contain the types of PKI certificates in Paragraphs 3A.1.e.(1)-(3) according to the specifications in Paragraphs 3A.1.e.(1)-(3):

(1) Authentication certificate.

The PKI authentication certificate on the staff support alternate token, special-purpose NSS PKI credential, or mobile PKI credential will support smart-card logon and will have the value of the supported U.S. GO/FO or SES user principal name field as an entry in the subject alternate name field of the certificate. Each credential will be issued to the individual or role identified in the common name field in the PKI certificates.

(2) Digital signature certificate.

The PKI digital signature certificate on the staff support alternate token, special-purpose NSS PKI credential, or mobile PKI credential will allow GO/FO and SES staff to digitally sign e-mails or documents on behalf of the GO/FO or SES. The staff members must not under any circumstances sign an e-mail or document as the GO/FO or SES. DoD Components must not issue U.S. GO/FO or SES staff a PKI certificate or credential (e.g., alternate token on NIPRNET)

asserting the identity of the GO/FO or SES, as this violates a fundamental principle of identity assurance.

(3) Encryption certificate.

The PKI encryption certificate on the staff support alternate token, special-purpose NSS PKI credential, or mobile PKI credential will allow GO/FO and SES staff to decrypt and read encrypted e-mails sent to the GO/FO or SES and to send encrypted e-mails on behalf of the GO/FO or SES. Unlike the digital signature certificate, the staff support encryption certificate is essentially a copy or clone of the GO's/FO's or SES's PKI encryption certificate.

f. The issuance of staff-support alternate tokens, special-purpose NSS PKI credentials, or mobile device PKI credentials as group authentication credentials will be conducted in accordance with the appropriate DoD Component CPS. This requires each DoD Component to verify that its CPS allows the issuance of U.S. GO/FO and SES staff support alternate tokens, special-purpose NSS PKI credentials, and mobile device PKI credentials as group authentication credentials.

3A.2. U.S. GO/FO AND SES CREDENTIAL REQUIREMENTS.

a. At all times, U.S. GOs/FOs and SESs must retain positive control and possession of their CACs, personal very important person credentials, DoD NSS PKI credentials, and/or any other PKI credential or certificate issued to them for their own use. GOs/FOs and SESs may not share their PKI credentials or personal identification number with other personnel, including their staff.

b. While GOs/FOs and SESs may be issued multiple personal very important person credentials, alternate tokens, or NSS PKI credentials, this practice is not recommended, as it increases the risk of a credential being lost, misplaced, given to a staff member, or otherwise being outside the positive control and possession of the GO/FO or SES. DoD Components may make their own risk decisions and determine how many, if any, of these additional PKI credentials may be issued to GOs/FOs and SESs based on documented mission need.

APPENDIX 3B: MISSION PARTNER EXTERNAL PKI APPROVAL PROCESS

3B.1. UNCLASSIFIED MISSION PARTNER AND COMMERCIAL VENDOR EXTERNAL PKI.

The DoD CIO oversees and facilitates the approval process for unclassified mission partner and commercial vendor PKIs. Approved unclassified mission partner PKIs must not be used to authenticate to classified networks and systems. Specific requirements for each type of PKI are summarized in Paragraph 3B.1.c.

a. Types of Unclassified Mission Partner and Commercial Vendor External PKIs.

(1) Federal Executive Branch Department and Agency PIV PKIs.

Some individual Federal Executive Branch departments and agencies operate their own PKIs and issue PIV PKI credentials to their personnel.

(2) Federal Executive Branch Shared Service Provider (SSP) PIV PKIs.

Some Federal departments and agencies contract PKI services under the GSA PKI SSP Program. Using the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework under the SSP Program, they can use services provided by the Federal PKI, participating commercial PKIs, or other Federal Executive Branch departments and agency PKIs to issue PIV PKI credentials to their personnel.

(3) Commercial Medium Hardware PKIs.

Commercial medium hardware PKI issuers are usually large DoD industry partners (e.g., aerospace partners). They usually issue their PKI credentials only to their employees and contractors, but they may issue PKI credentials to other organizations if their MOA with the DoD permits it.

(4) Commercial Personal Identity Verification-Interoperable (PIV-I) PKIs.

Commercial PIV-I PKI issuers are usually companies in the secure identity and authentication business. These companies issue PIV-I credentials to employees and contractors of other commercial organizations that would like to do business with the Federal Government but do not want to develop their own PKIs. This does not prevent these companies from issuing PIV-I credentials to their own personnel if their MOA permits this. PIV-I issuers also issue PIV-Is to State and local governments and non-executive Federal entities (e.g., the United States Senate).

(5) CCEB Partner PKIs.

Some CCEB partner nations operate their own unclassified PKIs and issue credentials to their personnel.

(6) Other Mission Partner External PKIs on Unclassified DoD Networks.

Other mission partners (e.g., non-CCEB foreign governments, group or multinational organizations such as the North Atlantic Treaty Organization) may seek approval for their PKIs on unclassified DoD networks.

b. Unclassified Mission Partner and Commercial Vendor External PKI Approval Criteria.

(1) Policy Mapping.

The mission partner or commercial vendor will provide policy-mapping documentation to the DoD PKI PMO, including compliance auditor documentation, so that the DoD PKI PMO can identify critical risks and potential impacts. The mission partner must show the DoD CIO that their requested CP OIDs are mapped to either:

(a) The medium hardware or high-assurance CP OIDs in the X.509 Certificate Policy for the Federal Bridge Certification Authority, either directly or through a PKI bridge cross-certificate issued by the Federal bridge CA;

(b) The common-hardware, common-authentication, or common-high CP OIDs in the X.509 Certificate Policy for the Federal Bridge Certification Authority; or

(c) The medium hardware assurance or above CP OIDs in the current edition of the U.S. DoD X.509 CP.

(2) Sponsorship.

In coordination with the relevant DoD Components, the DoD CIO must identify a business case or mission need for DoD to accept PKI credentials from the mission partner or commercial vendor external PKI. Federal PIV and SSP PIV PKIs do not require sponsorship.

(3) Interoperability Testing.

Upon request by the DoD CIO, the DISA JITC will test the mission partner or commercial vendor external PKI credentials and certificates for technical interoperability with DoD ISs, including web servers and e-mail clients, and verify that DoD ISs can receive certificate revocation status information. For CCEB-nation PKIs, the DoD CIO will work with JITC to facilitate whatever interoperability testing is necessary pursuant to Allied Communications Publication 185. For further information, see the JITC Website at http://jitc.fhu.disa.mil/projects/pki/index.aspx.

(4) Review.

The DoD CIO will review the business case or mission need, policy mapping, critical risk analysis, potential impacts, and interoperability testing results as necessary to determine whether the mission partner or commercial vendor external PKI presents an acceptable risk for use with

unclassified DoD systems and applications. Federal PIV and SSP PIV PKIs do not require review.

(5) MOA.

Commercial vendors, defense industry mission partners, and foreign mission partners must sign an appropriate agreement or arrangement with the DoD CIO. The DoD CIO will coordinate the MOA drafting and signature process with the mission partner and the Office of the General Counsel of the Department of Defense. MOAs for commercial vendors must include a provision to report any impending sale of part or all of the entity to the DoD CIO representative to the Committee on Foreign Investment in the United States. Federal PIV and SSP PIV PKIs do not require MOAs.

(6) Repository.

Once all parties sign the MOA, or JITC testing is successfully completed for Federal PIV and SSP PIV PKIs, the DoD CIO will notify the DISA that a new mission partner or commercial vendor PKI has been approved. Within 60 days of receiving this notification, the DISA must post the PKI's trust chain to the DISA repository for DoD-approved mission partner and commercial vendor external PKIs at https://cyber.mil/pki-pke/interoperability.

(7) Infrastructure Updates.

To maintain their status as partners in good standing, DoD-approved mission partners and commercial vendors must:

(a) Notify the DoD CIO and DISA whenever they deploy or rekey CAs for their DoD-approved PKIs.

(b) Update their MOA to reflect the new CAs if the DoD CIO review of the new CAs determines that this is necessary.

(c) Support additional JITC testing if the DoD CIO review of the new CAs determines that this is necessary.

(d) Provide the DISA with the information necessary to post the new PKI information to https://cyber.mil/pki-pke/interoperability.

c. Unclassified Mission Partner External PKI Mapping to Approval Criteria.

Table 1 indicates which approval criteria are required for which unclassified mission partner external PKIs.

Table 1. Mission Partner PKIs on DoD Unclassified Networks

Mission Partner or Commercial Vendor	Policy Mapping	Sponsor-ship	Interoperability Testing	Review	MOA	Repository
Federal Executive Branch Department and Agency PKIs	X	-	X	-	-	X
Federal Executive Branch Agencies Under the Federal SSP Program	X	-	X	-	-	X
Commercial Medium Hardware PKIs	X	X	X	X	X	X
Commercial PIV-I PKIs	X	X	X	X	X	X
CCEB Partner PKIs	X	X	X	X	X	X
Other Mission Partner PKIs	X	X	X	X	X	X

3B.2. SECRET FABRIC MISSION PARTNER EXTERNAL PKI.

The DoD CIO oversees and facilitates the approval process for secret fabric mission partner PKIs.

a. Federal Executive Branch Department and Agency PKIs.

CNSSP 25 requires all Federal Executive Branch departments and agencies to obtain certificates from the NSS PKI. Certificates issued by the NSS PKI, including the DoD NSS PKI, the NSS PKI Common Service Provider, and other agency NSS PKI CAs, are approved for use.

b. DoD-Cleared Contractors Accessing the SIPRNET from Contractor Sites.

Contractor PKIs are not approved for use on the SIPRNET. DoD contractors must obtain PKI certificates from the DoD NSS PKI and use these certificates to authenticate to SIPRNET resources regardless of the resource location. This requirement applies regardless of whether the cleared contractors are enrolled in the defense enrollment eligibility reporting system and regardless of whether the contractor-site SIPRNET connection operates in a Microsoft Active Directory environment.

c. CCEB Partner PKIs.

CCEB partner PKIs are approved for use on the DoD Secret Fabric if they meet the requirements in Paragraphs 3B.2.c.(1)-(6):

(1) Policy Mapping.

The CCEB partner must map their Secret Fabric PKI CP against the requirements specific in Allied Communications Publication 185 and identify any areas where their PKI does not meet Allied Communications Publication 185 requirements.

(2) Sponsorship.

The DoD PKI PMA is the sponsor for all CCEB-nation PKIs.

(3) Interoperability.

The DoD CIO will work with the DISA to facilitate interoperability testing for CCEB PKIs.

(4) Review.

The DoD CIO will review the policy mapping and interoperability testing results and consult with the Joint Staff and the DoD PKI PMO to determine whether the CCEB partner's Secret Fabric PKI is acceptable for the DoD Secret Fabric. The DoD and CCEB partner will cross-certify their Secret Fabric PKIs in accordance with the January 10, 2020 DoD CIO Memorandum for Five Eyes PKI and Allied Communications Publication 185.

(5) MOA.

The CCEB partner must sign a cross-CA with the DoD CIO. Once they sign an agreement, the DoD PKI PMO may direct DoD NSS PKI cross-certificates issuances to the CCEB partner's Secret Fabric PKI.

(6) Repository.

Once all parties sign the MOA, the DoD CIO will notify the DISA that a new mission partner PKI has been approved. Within 60 days of receiving this notification, the DISA must post the CCEB PKI's trust chain to the DISA repository for DoD-approved mission partner PKIs at https://cyber.mil/pki-pke/interoperability.

d. Other Mission Partner External PKIs.

Other mission partner secret fabric external PKIs (e.g., commercial on secret PKIs, non-CCEB foreign government PKIs, group or multinational PKIs such as the North Atlantic Treaty Organization PKI) are approved for use on DoD Secret Fabric networks if they meet these requirements:

(1) Policy Mapping.

The mission partner will provide policy-mapping documentation to the DoD PKI PMO, including compliance auditor documentation, so that the DoD PKI PMO can identify critical

risks and potential impacts. The mission partner must show the DoD CIO that their requested CP OIDs are mapped correctly to the CP OIDs in the DoD S-Interoperability Domain X.509 CP.

(2) Sponsorship.

A DoD Component or the DoD CIO must identify a business case or mission need to interoperate with the PKI.

(3) Interoperability.

The DoD CIO will work with the DoD PKI PMO to facilitate interoperability testing so the mission partner PKI can safely and securely authenticate DoD Secret Fabric resources, gateways, or demilitarized zones that the DoD may create.

(4) Review.

The DoD CIO will review the business case or mission need, policy mapping, critical risks, potential impact, and interoperability testing to determine whether the mission partner PKI presents an acceptable risk for the DoD Secret Fabric network.

(5) MOA.

All partner PKIs must carry out an appropriate MOA with the DoD.

(6) Repository.

Once all parties sign the MOA, the DoD CIO will notify the DISA that a new mission partner PKI has been approved. Within 60 days of receiving this notification, the DISA must post the PKI's trust chain to the DISA repository for DoD-approved mission partner PKIs at https://cyber.mil/pki-pke/interoperability.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AAL	authenticator assurance level
CA	certification authority
CAC	common access card
CCEB	combined communications-electronics board
CIO	chief information officer
CNSSD	Committee on National Security Systems directive
CNSSI	Committee on National Security Systems instruction
CNSSP	Committee on National Security Systems policy
CP	certificate policy
CPS	certification practice statement
CRL	certificate revocation list
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoDD	DoD directive
DoDI	DoD instruction
EA	executive agent
ECA	external certification authority
EEMSG	Enterprise Email Message Security Gateway
e-mail	electronic mail
FIPS	Federal information processing standard
GO/FO	general officer/flag officer
GSA	General Services Administration
ICAM	identity, credential, and access management
IS	information system
IT	information technology
JITC	Joint Interoperability Test Command
LRA	local registration authority
MDM	mobile device management
MOA	memorandum of agreement
MPE	mission partner environment

ACRONYM	MEANING
NEATS	NIPRNET Enterprise Alternate Token System
NIPRNET	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	non-person entity
NSA	National Security Agency
NSS	national security system
OID	object identifier
OLT	only locally trusted
PIV	personal identity verification
PIV-I	personal identity verification-interoperable
PKE	public key enabling
PKI	public key infrastructure
PMA	policy management authority
PMO	program management office
RA	registration authority
RAPIDS	Real-Time Automated Personnel Identification System
SES	senior executive service
SIPRNET	SECRET Internet Protocol Router Network
SP	special publication
SSP	shared service provider
TA	trusted agent
WCF	web content filter

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
AAL	AAL indicates the robustness of the authentication process itself and the binding between an authenticator and a specific individual's identifier. This term comes from NIST Special Publication (SP) 800-63-3. See NIST SP 800-63-3 for further information on AAL levels. The NIST SP 800-63-3 Website is at https://pages.nist.gov/800-63-3/.

TERM	DEFINITION
alternate token	A PKI credential issued for use on unclassified DoD networks and systems for specific situations where CACs are not used due to technical or policy reasons, such as authentication to IT privileged user–accounts; group, role, or watch officer accounts; and GO/FO or SES accounts by their staff. NEATS issues alternate tokens, which are sometimes also termed "NEATS tokens" or "NEATS alternate tokens." Alternate tokens were formerly termed "Alternate Logon Tokens" or "ALTs."
authenticator	Something the entity possesses and controls that is used to authenticate the entity and link it to the entity's digital identity. For example, for PKI, the authenticator is the private key that the entity uses to verify that the entity is associated with the digital identity in the public key certificate.
breach	Defined in Office of Management and Budget Memorandum M-17-12.
CA	Defined in CNSSI 1300.
CAC	Defined in CNSSI 4009. For further information on CACs, please see https://www.cac.mil/.
certificate	Defined in the DoD X.509 CP.
Certificate Policy Management Working Group	A working group chaired by the DoD PKI PMO that evaluates and recommends changes to DoD unclassified PKI, ECA PKI, and DoD NSS PKI CPs and CPSs.
coalition	A temporary alliance of distinct parties, persons, or -s for multinational action that may include any combination of mission partners.
code-signing certificate	A PKI certificate used to digitally sign mobile code, thereby certifying the mobile code as trustworthy.
common service provider	An organization or vendor that provides a service that issues any type of identity credential or identification card. Normally, the credentialing service outsources the production of identity credentials for an organization or entity that does not operate its own credentialing capability.

TERM	DEFINITION
controlled unclassified information	Defined in DoDI 5200.48.
cooperative program	Defined in DoDD 5230.20.
CP	Defined in CNSSI 1300.
CP OID	Defined in CNSSI 1300.
CPS	Defined in CNSSI 1300.
credential	An object or data structure that authoritatively binds a digital identity, via one or more identifiers and optionally additional attributes, to at least one authenticator that the entity associated with the digital identity possesses and controls. For example, a public key certificate is a credential that binds a digital identity to a public key.
cross-certification	The act or process by which one PKI extends trust to another PKI through issuance of a cross-certificate from a CA within the PKI extending trust to a CA within the PKI to which trust is being extended. Cross-certification enables DoD-relying parties to validate certificates from partner PKIs without installing the other PKIs' roots (i.e., without using direct trust). For example, the DoD unclassified PKI's cross-certification with the Federal bridge CA asserts that the DoD unclassified PKI operates in accordance with the standards, guidelines, and practices of the Federal PKI Policy Authority.
cryptography	Defined in NIST SP 800-59.
Defense Personnel Exchange Program	Defined in DoDD 5230.20.
direct trust	A simple mechanism of establishing trust of a PKI by installing its root CA, and intermediate CA certificates if required by the application, into the application's certificate trust store.
DoD-approved PKI	A PKI CA or overall infrastructure that the DoD CIO approves for use and acceptance by DoD-relying parties. DoD-approved PKIs include the DoD PKI, the ECA PKI, and certain external (e.g., mission partner) PKIs.

TERM	DEFINITION
DoD beneficiaries	Defined in DoDI 6010.23.
DoD IS	A DoD-owned, -managed, or -operated IS.
DoD NSS PKI	The DoD-operated portion of the NSS PKI used for authentication to DoD Secret Fabric networks and systems.
DoD NSS PKI certificate	A PKI certificate that the DoD NSS PKI issues.
DoD PKI	The DoD unclassified PKI, DoD NSS PKI, and other PKIs that the DoD PKI PMO runs.
DoD PKI interoperability	The ability of DoD-relying parties, such as web servers and e-mail users, to accept certificates that DoD-approved PKIs issue for authentication and to rely upon the authenticated identity as a basis for rules-based system, data authorization, or access control decisions.
DoD PKI PMO	A DoD office responsible for all aspects of the DoD unclassified PKI and the DoD NSS PKI that the NSA, DISA, and DMDC jointly manage. The NSA appoints the director of the DoD PKI PMO, and the DISA appoints the deputy program manager of the DoD PKI PMO.
DoD unclassified PKI	The DoD PKI for unclassified DoD networks and systems.
DoD unclassified PKI certificate	A PKI certificate that the DoD unclassified PKI issues.
DoD user	An individual person who has a legitimate need to access a DoD-owned or -operated network or system. To be considered a user, the individual must be in the process of applying for access to the DoD network or system in question or already have access.
ECA	The program DoD established to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations for use on unclassified DoD networks. The DoD established and controls the governing ECA CP. The issuing CAs are owned and operated by a commercial entity approved as meeting the DoD ECA CP and may create, sign, and issue certificates to external entities that DoD-relying parties may use for authentication, signature, and encryption.

TERM	DEFINITION
entity	Any person, role, organization, physical device, virtual device, or process that requests access to and uses resources. Entities are provided with credentials to verify their association with a digital identity, which consists of a unique identifier that may have additional attributes bound to it.
external PKI	A PKI that the DoD does not run and that provides PKI certificates for DoD mission partners to use on DoD networks and systems. ECAs, commercial vendor PKIs, and mission partner PKIs are types of external PKIs.
Federal Secret Fabric	Defined in CNSSD 507.
foreign liaison officer	Defined in DoDD 5230.20.
general users	Users who require access to information resources that the IS provides but do not have additional authorities within the IS.
hardware credential	A portable, user-controlled, physical device used to generate, store, and protect cryptographic information and to perform cryptographic functions. In the context of this policy, a PKI hardware credential is a physical device or form factor to which PKI certificates are bound, because they were created and stored on the device (e.g., the CAC).
intermediate CA	Defined in CNSSI 1300.
IS	Defined in DoD the ICAM Reference Design.
IT privileged user	A user who has roles that allow read, write, or change access to manage IT systems, including system, network, and database administrators, as well as security analysts who manage audit logs. IT privileged user roles are generic to all IT infrastructure, including transport, DoD and commercial clouds, hosting environments, cybersecurity, and application deployment.
key recovery	The capability for authorized entities to retrieve keying material from a key backup or archive. Recovery of an individual's escrowed encryption key (keying material) initiated by the individual issued that encryption key is a first-party key recovery process. The individual is always authorized to recover their own escrowed private keys. Recovering an individual's escrowed encryption key initiated by someone other than the individual that the key was issued to is a third-party key recovery. Third parties must obtain authorization to receive someone else's escrowed private key.

TERM	DEFINITION
mission partner	Defined in the DoD ICAM Reference Design.
mobile code	Defined in CNSSI 4009.
MPE	Defined in DoDI 8110.01.
NEATS	A centralized token management system for DoD PKI certificates on NEATS alternate tokens, also known as "alternate tokens," for use cases to include administrators, groups, roles, code signing and individuals not authorized to receive a PIV (e.g., a CAC).
network	Defined in CNSSI 4009.
network account	An account on a DoD network that is assigned to a specific individual user and that grants the user access to local domain resources, such as SharePoint, share drives, printers, Windows applications, and e-mail. Network accounts are usually tied in some fashion to the Microsoft Active Directory.
NPE	A physical device, virtual machine, system, service, or process that is assigned an identifier and is issued credentials to support authentication and authorization. NPEs authenticate to ISs independent of individual actions by person entities. NPEs may be acting on behalf of a person entity, such as robotic process automation bots, but must be independently authorized to perform any actions. Any resource that authenticates itself to person entities or other NPE resources including web browsers is an NPE. NPEs may also be resources, but resources that do not themselves authenticate themselves to person entities or other resources are generally not considered NPEs. For additional information, please see the DoD ICAM Reference Design.
NPE PKI certificate	These certificates, usually software certificates, securely and reliably authenticate devices to other devices and users. They also facilitate Secure Sockets Layer/transport layer security connections, or other cryptographically secure connections, among the devices and users (or other devices) for purposes of the secure exchange of information. These NPE PKI certificates are alternately termed "server certificates," "software certificates," or "Secure Sockets Layer/transport layer security certificates."
OID	A value, distinguishable from all other such values, that is associated with an information object.

TERM	DEFINITION
person entity	An individual acting as themselves or in the capacity of a role that is assigned an identifier and attributes, issued credentials, and provided with entitlements to support authentication and authorization. Person entities include named individuals, organization roles (e.g., acting on behalf of an executive), and job function roles (e.g., IT privileged users).
personally identifiable information	Defined in Office of Management and Budget Circular A-130.
PIV	Defined in CNSSI 4009.
PKE	Defined in CNSSI 4009.
PKI	Defined in the DoD ICAM Reference Design.
registration practice statement	Defined in CNSSI 1300.
relying party	Defined in CNSSI 1300.
root CA	Defined in CNSSI 1300.
smart card	A credit card–sized device containing one or more integrated circuits that may employ at least one magnetic stripe, bar code (linear or two dimensional), non-contact and radio frequency transmitters, biometric information, encryption and authentication information, or photo identification.
special-purpose DoD NSS PKI credentials	DoD NSS PKI hardware credentials can be configured for special purposes similar to what Alternate Tokens are used for on unclassified DoD networks. These special purposes include, but are not limited to: IT Privileged User Accounts; Group, Role, or Watch Officer Accounts; and U.S. GO, FO, and SES Staff Accounts.
SSP	An organization that provides PKI services and digital certificates for use by Federal agency employees and selected contractors pursuant to NIST FIPS Publication 201-2. The PKI SSP Program, which the GSA administers, was established to assist agencies with selecting a PKI service provider.
system owner	Defined in CNSSI 4009.

TERM	DEFINITION
transport layer security	Defined in CNSSI 4009.
U.S. Coalition PKI	The PKI used for authentication to DoD MPE networks and systems.
U.S. Coalition PKI certificate	A PKI certificate that the U.S. Coalition PKI issues.
user	Defined in CNSSI 4009.
watch officer	An officer who stands a watch.
web server	An automated IS that manages a website by passing web pages to web browsers over a network. The web server may provide information stored locally on the server or may act as a portal to allow the access of information from other linked ISs.

REFERENCES

Allied Communications Publication 185, "Public Key Infrastructure (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations," November 2011, as amended

Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum, "Assignment of Program Management Office Responsibilities for the Department of Defense Public Key Infrastructure (PKI)," April 9, 1999[1]

Committee on National Security Systems Directive 506, "National Directive to Implement Public Key Infrastructure on Secret Networks," January 11, 2019

Committee on National Security Systems Directive 507, "National Directive for Identity, Credential, and Access Mgmt. Capabilities on the U.S. Federal Secret Fabric," July 7, 2020

Committee on National Security Systems Instruction 1300, "Instruction for Secret National Security Systems Public Key Infrastructure X.509 Certificate Policy Under CNSS Policy No. 25," current edition

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," current edition

Committee on National Security Systems Policy 25, "National Policy for Public Key Infrastructure in National Security Systems," December 11, 2017

Defense Information Systems Agency, "Releasable Embedded Local Area Network Security Technical Implementation Guide (STIG) Overview," current edition[2]

DoD Chief Information Officer Memorandum, "DoD Mobile Public Key Infrastructure (PKI) Credentials," December 20, 2019

DoD Chief Information Officer Memorandum, "Requirement for the Five Eyes Nations to Establish Public Key Infrastructure Interoperability with DoD Classified Networks," January 10, 2020

DoD Directive 5101.22E, "DoD Executive Agent (DoD EA) for DoD Mission Partner Environment (MPE)," August 5, 2020

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

DoD Enterprise Identity, Credential, and Access Management, "DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design," Version 1.0, June 2020

DoD Instruction 1000.13, "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals," January 23, 2014, as amended

DoD Instruction 1000.25, "DoD Personnel Identity Protection (PIP) Program," March 2, 2016

DoD Instruction 1000.30, "Reduction of Social Security Number (SSN) Use Within DoD," August 1, 2012, as amended

[1] Available on request by e-mailing the DoD CIO ICAM team mailbox at osd.mc-alex.dod-cio.mbx.icam@mail.mil.
[2] Available on the Internet at https://dl.cyber.mil/stigs/zip/FOUO_REL_Embedded_LAN_V2R2_STIG.zip.

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5530.03, "International Agreements," December 4, 2019

DoD Instruction 6010.23, "DoD and Department of Veterans Affairs (VA) Health Care Resource Sharing Program," February 3, 2022

DoD Instruction 8110.01, "Mission Partner Environment Information Sharing Capability Implementation for the DoD," June 30, 2021

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 13, 2011, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021

Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended

Federal Information Processing Standards Publication 140-3, "Security Requirements for Cryptographic Modules," March 22, 2019

Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004

Federal Information Processing Standards Publication 201-2, "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013

Federal Public Key Infrastructure Policy Authority, "X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)," current edition

Federal Public Key Infrastructure Policy Authority, "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework," current edition

General Services Administration and Federal Chief Information Officers Council, "Use of Electronic Signatures in Federal Organization Transactions," Version 1.0, January 25, 2013

Homeland Security Presidential Directive-12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004

Joint Interoperability Test Command Website, "Public Key Infrastructure (PKI)," http://jitc.fhu.disa.mil/projects/pki/index.aspx

Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017

National Institute of Standards and Technology Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System," August 2003

National Institute of Standards and Technology Special Publication 800-63-3, "Digital Identity Guidelines," June 2017, as amended

Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016

Office of Management and Budget Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," January 3, 2017

United States Coalition X.509 Certificate Policy, current edition[3]

United States Cyber Command Tasking Order 14-0018, Technical Attachment 1, "Actions to Mitigate Microsoft Windows Credential Theft Vulnerabilities," January 28, 2014[4]

United States Department of Defense External Certification Authority X.509 Certificate Policy, current edition[5]

United States Department of Defense S-Interoperability Domain X.509 Certificate Policy, Version 1, January 5, 2012[6]

United States Department of Defense Web Content Filter X.509 Certificate Policy, Version 1, October 10, 2019[7]

United States Department of Defense X.509 Certificate Policy, current edition

[3] Available on request by e-mailing the DoD CIO ICAM team mailbox at osd.mc-alex.dod-cio.mbx.icam@mail.mil.
[4] Available on request by e-mailing the DoD CIO ICAM team mailbox at osd.mc-alex.dod-cio.mbx.icam@mail.mil.
[5] Available on the Internet at https://dl.cyber.mil/pki-pke/pdf/unclass-dod_eca_cp-v4_5-20190220.pdf.
[6] Available on the Internet at https://dl.cyber.mil/pki-pke/pdf/unclass-dod_s-interop_domain_x509_cp_v1_5jan12.pdf.
[7] Available on request by e-mailing the DoD CIO ICAM team mailbox at osd.mc-alex.dod-cio.mbx.icam@mail.mil.