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

OCT 24 2025

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

SUBJECT: Multi-Factor Authentication (MFA) for Unclassified & Secret DoD Networks

References: (a) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key Enablement (PKE)," May 18, 2023
(b) DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 19, 2023
(c) Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021
(d) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990

DoD Instruction (DoDI) 8520.02, "Public Key Infrastructure (PKI) and Public Key Enablement (PKE)," (reference a) and DoDI 8520.03, "Identity Authentication for Information Systems," (reference b) establish DoD-approved PKI as the principal and preferred "means of authenticating persons to Department of Defense (DoD) systems and applications." Reference (b) also authorizes the use of DoD-approved non-PKI methods of Multi-Factor Authentication (MFA) when DoD-approved PKIs are impractical or infeasible. This memorandum establishes DoD non-PKI MFA policy and identifies DoD-approved non-PKI MFAs based on use cases.

This memorandum replaces Section 3.3 and modifies Section 3.5 of DoDI 8520.03. Specifically, Attachment 1 updates the process for determining the method of authentication required for users to access DoD resources. Attachment 2 provides the current list of DoD-approved non-PKI MFAs, Attachment 3 provides general non-PKI MFA implementation requirements, and Attachment 4 lists DoD-approved non-PKI MFA use-cases and provides supplemental implementation requirements for those use-cases. The contents of Attachments 1 and 3 of this memorandum will be incorporated into DoDI 8520.03 within 12 months of signature of this memorandum, while Attachments 2 and 4 will be made available to the DoD community and updated when new use-cases or exceptions are approved per the process in Attachment 2.

This memorandum applies to users (privileged/non-privileged individuals, organizational roles, and job function roles) authenticating to unclassified and Secret Fabric DoD information systems and environments, regardless of hosting location, and does not apply to digital-signing and encrypting e-mails or documents. This memorandum also does not apply to: DoD information cleared for public release, Non-Person Entities, or cryptographic products/solutions Certified or Approved by the National Security Agency under National Security Directive 42 (reference (d)) (e.g., High Assurance cryptographic products, commercial solutions for classified). This policy memorandum supersedes previous non-PKI MFA DoD CIO approval memorandums. DoD CIO

memorandums approving Identity Federation Services (IFS) are not impacted. Existing exceptions to policy (E2P) for non-PKI MFAs will remain in force until they expire.

The point of contact for this memorandum is Mrs. Patricia Janssen at patricia.l.janssen.civ@mail.mil or (571) 372-4221.

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Attachments:
As stated

Attachment 1: Policy Updates

DoDI 8520.03 uses Risk Management Framework (RMF) Confidentiality Risk Levels to determine when and under what circumstances users may authenticate to DoD resources with methods other than DoD-approved PKI. This policy replaces the RMF Risk levels as the means to determine permitted methods of authentication. Instead, regardless of the RMF risk level, the following rules apply for authentication to DoD unclassified and Secret Fabric networks, systems, applications, devices, information, or cloud environments and commercial internet service provider connections:

1) DoD-approved PKI, as defined in DoDI 8520.02, is the primary and preferred means of authentication for DoD information and resources on both unclassified and Secret Fabric DoD networks. Authorizing Officials (AO) may not authorize the use of a PKI that has not been approved by the DoD CIO or otherwise provided for in DoDI 8520.02.[1]

2) DoD-approved non-PKI MFA[2] implemented in accordance with this policy are the immediate fallback if DoD-approved PKI cannot be used. There are two circumstances under which an Authorizing Official (AO) may authorize the use of a non-PKI MFA:

    a. The AO determines that the system or application owner has provided them sufficient evidence and documentation for the AO to verify the use-case aligns with a DoD-approved non-PKI MFA Use-Case. The AO then approves the use of a DoD-approved non-PKI MFA in line with its rules and restrictions, and ensures it is implemented in accordance with the requirements for that particular use-case.
    b. The AO determines DoD-PKI is infeasible, approves the use of a DoD-approved non-PKI MFA in line with that MFA's rules and restrictions, and ensures the DoD-approved non-PKI MFA is implemented in accordance with Attachment 3.
        i. To determine that DoD-approved PKI is infeasible, the AO must determine that the system or application owner has provided them with sufficient evidence and documentation for the AO to verify that **either:**
            1. The device or user environment the user is authenticating from or to presents technical limitations preventing the use of DoD-approved PKI for authentication purposes (DoD-approved PKIs include CAC, ALT, ECAs, NSS SIPR PKI tokens, or any of the DoD-approved PKIs listed on https://cyber.mil/pki-pke/interoperability/).
            2. A portion of the system's users are unable to obtain or use DoD-approved PKI without great cost or hardship (e.g., beneficiaries who would need to bear the cost of purchasing external certificate authority (ECA) PKI certificates from their own personal funds, as opposed to a business which purchases ECAs for its employees).

3) In accordance with Executive Order 14028, Authorizing Officials (AOs) may no longer authorize the use of single factor authentication (e.g., only username and password). The only exceptions will be when single-factor authentication is specifically permitted in a particular DoD-approved use-case (e.g., Emergency Accounts use-case in Attachment 4).

[1] For DoD-approved PKIs, please see https://cyber.mil/pki-pke/interoperability/ & https://cyber.mil/eca/.
[2] For DoD-approved non-PKI MFAs, please see Attachment 2 of this memorandum.

When authorizing the use of DoD-approved non-PKI MFAs, AOs must ensure:

1. Where operationally feasible (e.g., the information system has connectivity to the DoDIN or commercial internet), the system requires PKI authentication for all users capable of obtaining and using DoD-approved PKIs (e.g., if a system has both DoD users with CACs and beneficiary users who are ineligible for CACs, then it still must support CAC-authentication for the CAC-holders while allowing the beneficiaries to authenticate with a DoD-approved non-PKI MFA).

2. If the non-PKI MFA (or any other DoD-approved method of authentication) is to be used in a commercial cloud environment, the cloud service offering (CSO) must either have a Provisional Approval (PA) from DISA or another type of approval that meets the requirements of the Defense Information Systems Agency (DISA) DoD Mission Owner and Cloud Service Provider Security Requirement Guide (SRG). This applies regardless of whether the user possesses the credential, or the credential is hosted in the CSO. CSOs that are outside DoD boundaries and do not store, transmit, or process DoD data, such as certain USCG CSOs, may have a FedRAMP certification in lieu of a DISA Cloud PA.

3. The non-PKI MFA Capability is integrated with a DoD-approved ICAM service provider (SP) in accordance with the DoD CIO memorandum of May 17, 2023, "Adoption of Initial ICAM Enterprise Services." (this requirement does not apply to DoD-approved non-PKI MFAs being used in a DDIL, stand-alone, or commercial ISP environment).

Attachment 2: DoD-approved Non-PKI MFAs & Approval Process

The following non-PKI MFAs are DoD-approved when used as part of an MFA solution. This list is expected to be a living document and will be posted at: https://intelshare.intelink.gov/sites/dodcioicamdocs. The list will be updated as new MFAs (and MFA versions) are approved and other MFAs are removed due to evolving security risks. For purposes of choosing and using a non-PKI MFA, functional privileged users[3] will abide by the same rules and restrictions for unprivileged users accessing CUI, or IL4 or IL5 cloud environments (or unprivileged users authenticating to DoD Secret Fabric systems and IL6 environments).

Issuer	**Credential/ Authenticator**	**Rules**	**Restrictions**
Defense Manpower Data Center (DMDC)	myAuth[4] (supports various non-PKI MFAs)	- DoD Components are encouraged to use DMDC myAuth to facilitate identity-proofing for users without DoD-approved PKI credentials. - If the authenticator that myAuth is being used with is approved, then myAuth paired with that authenticator is approved subject to the same rules and limitations.[5] - Non-PKI MFAs supported by myAuth, but not addressed in this policy (e.g., Okta Verify MFA Push or Okta Verify MFA OTP) are only approved to access Cloud Impact Level (IL) 2 environments, low risk information, and the user's own PII and PHI (e.g., beneficiary use-case).	- Not approved to access DoD CUI and IL4/IL5 cloud environments **unless** used with Okta Verify MFA with Cryptographic FastPass (or DoD-approved PKI). - Not approved for the DoD Secret Fabric or other classified networks or cloud environments. - Not approved for IT Privileged User Accounts.[6]
US Army & Air Force	MobileConnect MFA	- Approved for access to data up to (and including) CUI, regardless of whether the data is hosted in an IL2, IL4, or IL5 cloud environments.	- Not approved for the DoD Secret Fabric or other classified networks or cloud environments. - See Attachment 4 for IT Privileged User use-cases.
RSA	HW SecurID Tokens	- Approved for access to data up to (and including) CUI,	- Also approved for authentication to DoD Secret

[3] A Functional Privileged User has approval authorities within workflows. Functional privileged user roles are specific to a mission area, such as human resources or finance.

[4] DS-Logon is temporarily approved for users or beneficiaries accessing their own PII and IL2 information until these users can transition to myAuth. DS-Logon is planned for decommissioning by the end of CY2026.

[5] For example, myAuth with Okta Verify MFA with Cryptographic FastPass is approved subject to the same rules and restrictions for that MFA, and myAuth with SMS OTP is allowed when SMS OTP is allowed.

[6] An IT Privileged User is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. IT privileged users include system, network, or database administrators, security administrators, developers, configuration managers, release managers, and security analysts who manage audit logs.

Issuer	Credential/ Authenticator	Rules	Restrictions
		regardless of whether the data is hosted in an IL2, IL4, or IL5 cloud environments.	Fabric systems, applications, devices, or cloud environments, provided user first logs onto the Secret network with DoD-approved PKI (e.g., DoD NSS SIPR PKI token). - See Attachment 4 for IT Privileged User use-cases.
Yubico	YubiKey – CTAP1/U2F & CTAP2/FIDO2 Passkey functions[7]	- Yubikeys must be approved at FIPS-140-2 or 140-3 level 1 to be used for non-PKI MFA. - Approved for access to data up to (and including) CUI, regardless of whether the data is hosted in an IL2, IL4, or IL5 cloud environments.	- Other Yubikey non-PKI MFA authentication functions are NOT DoD-approved. - Also approved for authentication to DoD Secret Fabric systems, applications, devices, or cloud environments, provided user first logs onto the Secret network with DoD-approved PKI. - See Attachment 4 for IT Privileged User use-cases.
SafeNet	e-Token Pass 3000 & 110 OTP Token	- Approved for access to data up to (and including) CUI, regardless of whether the data is hosted in an IL2, IL4, or IL5 cloud environments.	- Also approved for authentication to DoD Secret Fabric systems, applications, devices, or cloud environments, provided user first logs onto the Secret network with DoD-approved PKI. - See Attachment 4 for IT Privileged User use-cases.
Okta	Verify MFA with Cryptographic FastPass	- Approved for access to data up to (and including) CUI, regardless of whether the data is hosted in an IL2, IL4, or IL5 cloud environments. - Abide by Okta IDaaS STIG.	- Not approved for the DoD Secret Fabric or other classified networks or cloud environments. - See Attachment 4 for IT Privileged User use-cases.
Microsoft (MS)	Passkey in Microsoft Authenticator (TAP may be used for device	- Approved for access to data up to (and including) CUI, regardless of whether the data is hosted in an IL2, IL4, or IL5 cloud environments.	- Not approved for the DoD Secret Fabric or other classified networks or cloud environments.

[7] YubiKeys may also be used with DoD Purebred PKI certificates on unclassified DoD networks in accordance with the 2019 DoD Mobile PKI Requirements memo (https://dodcio.defense.gov/Portals/0/Documents/Cyber/DoDCIOMem-MobilePKICredentials.pdf). Please note that all FIPS-approved YubiKeys which meet the requirements in the 2019 memo are approved for Purebred on unclassified networks, not just the YubiKey 4 devices.

Issuer	Credential/ Authenticator	Rules	Restrictions
	registration only)		- See Attachment 4 for IT Privileged User use-cases.
Imprivata	iAccess Tap & Go	- Only approved for Medical Device use-case (Attachment 4).	- Not approved for the DoD Secret Fabric or other classified networks or cloud environments. - Not approved for IT Privileged User Accounts.
Swivel Secure	Swivel Secure MFA	- Only approved for use on the Sensitive Unclassified Network (SUNet), which is a separate network from the NIPRNet.	- Not approved for the DoD Secret Fabric or other classified networks or cloud environments. - Not approved for IT Privileged User Accounts.

Approval Process for Additional MFAs, Use-Cases, and Implementations

All five steps of the following process will be used for approval of all non-PKI MFAs, non-PKI MFA use-cases, or non-PKI MFA implementations not addressed in this policy:

1. **Component Approval**: All requests to approve a non-PKI MFA shall initially be brought by the requestor to their Component's Chief Information Security Officer (CISO) for validation. In particular, the Component CISO, shall validate the need for the product in light of existing DoD-approved PKI and non-PKI MFA options and the DoD-approved use-cases in this policy.

2. **Submit Exception to Policy (E2P)**: If the DoD Component's CISO validates the request, the requester shall submit a request to the Office of the DoD Chief Information Officer (DoD CIO) Exception to Policy (E2P) portal at https://rmfks.osd.mil/DoDE2P.

3. **Initial Review**: DoD CIO will evaluate the request against the implementation requirements in this policy, as well as other requirements and standards it may deem appropriate, such as degree of phishing-resistance and FIPS-140 or NIAP validation.

4. **Review by DoD ICAM Governance Bodies**: DoD CIO may facilitate reviews by DoD ICAM governance bodies (e.g., ICAM Configuration Control Board (CCB), Joint Integration Council (JIC) or Executive Board (IEB)).[8] As part of this process, DoD CIO may request additional information from the requester and that the request undergo a security assessment and testing from the National Security Agency (NSA).

5. **Decision**: The DoD Chief Information Security Officer (CISO), on behalf of DoD CIO, will decide whether to approve/disapprove the request for use of the non-PKI MFA, non-PKI MFA use-case, or non-PKI MFA implementations not addressed in this policy. Reasons for disapproval include, but are not limited to, non-responses to requests for additional information or documentation, insufficient reasons for not using DoD-approved PKI,

[8] See DoD CIO Memorandum, "Identity, Credential, and Access Management Governance Structure," May 17, 2023.

unacceptable security risks, and insufficient security mitigations. All approvals will be posted to: https://intelshare.intelink.gov/sites/dodcioicamdocs/. Any denials will be communicated directly to the requestor, along with rationalization for the denial. The requestor will then have the opportunity to re-submit after addressing issues identified in the denial.

Attachment 3: DoD-Approved Non-PKI MFA Implementation Requirements

DoD Credential Service Providers (CSP)[9] must implement DoD-approved non-PKI MFAs either in accordance with this attachment or, if applicable, the modified requirements for the use-cases in Attachment 4. For purposes of this policy, a DoD CSP is any DoD Component, Community of Interest (COI), or local information system issuing DoD-approved non-PKI MFAs to its users or having an agreement with another entity to issue DoD-approved non-PKI MFAs on its behalf. In the latter case, the CSP must ensure DoD-approved non-PKI MFAs are being implemented in accordance with this policy. Non-PKI MFA implementation requirements are divided into three categories: Credential Lifecycle, Authentication Strength, and Access Management.

A. Credential Lifecycle Requirements

1) **Identity-Proofing**: DoD CSPs must verify the identity of a user prior to issuing them a credential. Except for certain approved use-cases in Attachment 4, NIST SP 800-63A[10] Identity Assurance Level (IAL) 2 is the minimum identity-proofing required for non-privileged users (i.e., general users) accessing non-public DoD information. IAL-2 plus in-person identity-proofing with a trained CSP representative is the minimum identity-proofing required for Functional and IT privileged users. In addition, and depending on whether the user has a DoD-approved PKI credential, the CSP's identity-proofing must comply with the requirements in one of the two following sections:

   a) **Identity-proofing for Users with DoD-approved medium hardware assurance and above PKI Credentials (e.g., CAC Holders, DoD NSS SIPR PKI Token Holders)**.[11] Users may obtain a non-PKI MFA through electronic validation of DoD-approved hardware PKI credentials. These non-PKI MFAs are considered "derived" credentials. Please note, while the IAL of the derived non-PKI MFA credential is the same as the original PKI credential, the Authenticator Assurance Level (AAL) of the non-PKI MFA is usually weaker than the original PKI credential.[12] CSPs must do the following when issuing derived non-PKI MFAs:
      i) Require users to authenticate with their PKI credential to enroll their non-PKI MFA or to switch to using another non-PKI MFA.
      ii) Maintain a record of an identifier from the **original** credential (e.g. DoD ID Number, certificate serial number) and link it to the issuance of a non-PKI MFA credential and to the non-PKI MFA credential itself via an immutable characteristic or attribute.
      iii) Maintain a record of an identifier for the **derived** credential. If applicable, the CSP should also maintain a record of the device serial number in use.

[9] For purposes of this document, CSP stands for DoD Credential Service Provider, not cloud service provider.
[10] All references in this document to NIST SP 800-63 are to NIST SP 800-63-4 (https://pages.nist.gov/800-63-4/). In instances where the NIST policy and this DoD policy contradict, follow this DoD policy.
[11] This section updates Section 3.5.b.(2)(a) of DoDI 8520.03. "DoD-approved medium hardware assurance and above PKI credentials" includes many of the credentials listed at https://cyber.mil/pki-pke/interoperability/, as well as ECA Medium Hardware and ECA Medium Hardware PIV-I assurance credentials. It excludes ECA Medium assurance and Medium Token assurance credentials and derived DoD-approved PKI credentials like Purebred PKI (i.e., a non-PKI MFA cannot be derived from a derived PKI). Non-PKI MFAs may not be derived from other non-PKI MFAs.
[12] IALs relate to the identity-proofing process done before being issued a credential, whereas AALs relate to the strength of the credential itself. For example, for DoD purposes the CAC is considered IAL-3 and AAL-3. A non-PKI MFA derived from a CAC would likely be considered IAL-3 and AAL-2.

iv) Maintain a record of the binding of the DoD-approved PKI credential to the non-PKI MFA credential identifier.

v) Not distribute or encode the identifier of the DoD-approved PKI credential used for identity-proofing outside the CSP. The identifier for the derived non-PKI MFA credential and its associated device may be shared.

b) **Identity-proofing for Users Without DoD-approved PKI credentials (**e.g., non-CAC Holders, including foreign nationals who can't obtain DoD-approved medium hardware assurance or above PKI credentials**)**. This section is only applicable to unclassified networks and is not applicable to the DoD Secret Fabric. These users must identity-proof via one of the following before being issued a DoD-approved non-PKI MFA:

i) **Documentation Based Identity-Proofing.**[13] Identity proofing based on remote or in-person presentation of existing identity documents, such as a passport, driver's license, or other government-issued identity credential.[14] At least one of the documents used for identity proofing must contain a photograph of the person. In addition, the individual reviewing the documents must be familiar enough with the type of documents being presented to verify key anti-tamper features of the documents.

(1) Whenever possible, DoD CSPs should use DMDC myAuth to facilitate documentation-based identity-proofing on unclassified networks. If they don't have the manpower or infrastructure to perform identity-proofing using their own personnel, DoD Components may also use outside services (e.g., login.gov, ID.me), to perform documentation-based identity proofing, provided those services have been evaluated and certified by a separate independent organization (e.g., Kantara) as meeting NIST SP 800-63A IAL-2 requirements. The CSP must ensure the independent organization does a re-evaluation and re-certification of the outside service as meeting at least IAL-2 requirements once every three years.

ii) **Third-party Vouching.**[15] The CSP may rely on a trusted representative of DoD or a third-party organization (e.g., representative of a state, local, or foreign government) to vouch for and identity-proof third-party users who need limited access to unclassified DoD resources. Credential issuance, maintenance, and revocation processes described later in this attachment may not be feasible when third-party vouching is necessary.

(1) **Vetting:** The DoD or third-party representative who will be ID-proofing or registering third-party users, and/or issuing authentication credentials to these users, must provide all of the following to the DoD CSP:

(a) Evidence that they are a member or representative of the DoD or third-party organization. Third-party representatives must also provide evidence or reliably attest to an existing relationship between their organization and the CSP.

(b) Proof of their own identity through either DoD-approved PKI credential-based identity-proofing or documentation-based identity-proofing.

[13] This section replaces Section 3.5.b.(3) of DoDI 8520.03.

[14] Identity proofing based on presentation of documentation can meet IAL-2 or IAL-3 depending on which of the requirements in NIST SP 800-63A are met.

[15] This section replaces Section 3.5.b.(4) of DoDI 8520.03.

(c) A written description of how they are identity-proofing and monitoring credential issuance and revocation for third-party users. The CSP has the authority to instruct the representative to make changes to these processes.
(i) A verbal description may be used in an emergency or disaster situation where time or lack of resources prevents transmission of a written description. In this case, the CSP will document what the representative has told them.

(2) **Limitations:** Third-party vouching:
(a) May only be used when:
(i) Due to the location of the users or the urgency of the need, the DoD CSP does not have the onsite resources on-site resources for credential or documentation-based identity proofing and cannot find a reliable commercial organization to perform these services.
(ii) Certain limited populations, such as:
1. First responders and coalition partner representatives need access to specific unclassified DoD systems or portals to support emergency response or disaster recovery.
2. Foreign users from a variety of countries need limited access to unclassified training or foreign military sales (FMS) systems.
(b) May not be used for:
(i) Network access on unclassified DoD networks unless the network is a closed coalition or emergency responder network (i.e., not NIPRNet).
(ii) Broad access to DoD systems unrelated to the immediate need.
(iii) Access to IT privileged-user or functional privileged-user accounts.
(iv) Access to classified networks or systems.

2) **Credential Issuance:**[16]
a) For users who do not have an established DoD digital identity, CSPs must create unique identifiers for that individual user. These identifiers must be unique across the DoD, and not conflict with 10-digit DoD Electronic Data Interchange Personal Identifiers (EDIPI) or EDIPI plus 6 (16-digit Federal Agency Smart Credential Numbers (FASCN)).
b) CSPs must generate credentials containing or which are associated with the user's unique identifier.
c) CSPs must provide the credential using a process preventing anyone other than the user from accessing the authenticator. The CSP must inform the user that once they are issued the authenticator, they are responsible for ensuring that the authenticator is only accessed by the user for whom it is intended.
d) The CSP must bind the credential to the user's account(s) in accordance with the requirements in Section 4.1, "Authenticator-binding", of NIST SP 800-63B.
e) If needed, renew non-PKI MFAs in accordance with Section 4.1.4 of NIST SP 800-63B, with the caveat that the following adjusted DoD requirements must be followed:
i) The subscriber **must** bind a new or updated authenticator before an existing authenticator's expiration (NIST policy says SHOULD).
ii) The process for this **must** conform closely to the binding process for an additional authenticator, as described in Sec. 4.1.2 (NIST policy says SHOULD).

[16] This section replaces Section 3.5.c. of DoDI 8520.03.

iii) Following the successful use of the replacement authenticator, the CSP **must** invalidate the expiring authenticator (NIST policy says SHOULD).

3) **Credential Maintenance & Revocation:**[17] CSPs must:
   a) Track DoD systems, applications, or cloud environments where the user has registered and is using their non-PKI MFA.
   b) Use appropriate behavior analytics to ensure the non-PKI MFA is not compromised.
   c) Disable credentials not being used at their expected periodicity. CSPs will determine the period based on the expected frequency of use.
   d) Comply with DoD or DoD Component account management policies.
   e) Establish a help-desk service for non-PKI MFA users to report lost or stolen credentials, and a self-service portal where these users can delete their registered non-PKI MFAs.
   f) Provide a mechanism for account recovery in accordance with Section 4.2 of NIST SP 800-63B.
   g) Develop and implement procedures to suspend or revoke non-PKI MFAs or user accounts associated with non-PKI MFAs which the CSP, DoD Component, or their representative has reason to believe is compromised based on behavior analytics and other Zero Trust data.
   h) Revoke, disable, or invalidate lost, stolen, damaged, compromised, or duplicated credentials or authenticators promptly in accordance with Sections 4.3 and 4.5 of NIST SP 800-63B, with the caveat that the following adjusted DoD requirement must be followed:
      i) CSPs **must** establish time limits for revoking, disabling, or invalidating these credentials upon notification of a loss, theft, damage, compromise, or duplication.
   i) Ensure ALL non-PKI MFAs have an expiration date not more than one year after the authenticator was issued, except for the DoD Beneficiary Use-Case in Attachment 4, which shall have an expiration date of no more than two years.[18]
   j) Revoke, disable, or invalidate non-PKI MFA authenticators when they expire in accordance with Section 4.4 of NIST SP 800-63B, with the caveat that the following adjusted DoD requirement must be followed:
      i) CSPs **must** bind authenticators that expire to subscriber accounts.
   k) The user may rebind a current authenticator to their account before it expires, or rebind an expired authenticator to their account, if they first authenticate to their account with either a different DoD-approved non-PKI MFA or a DoD-approved hardware PKI.
   l) If a user obtains a "derived" non-PKI MFA through electronic validation of a DoD-approved hardware PKI credentials in accordance with paragraph A.1)a), then:
      i) If the DoD-approved PKI expires, or is revoked because it was lost or stolen, then all non-PKI MFAs derived from (and therefore linked) to that PKI credential must be suspended until the user is issued a new DoD-approved PKI credential. If the DoD-approved PKI credential is renewed within 45 days of the expiration or loss, the user's non-PKI MFAs may be unsuspended and bound to the user's new DoD-approved PKI credential. If the DoD-approved PKI credential is not renewed within 45 days, then all non-PKI MFAs derived from that PKI will expire.
      ii) If the DoD-approved PKI is revoked for cause (e.g., employee termination), then all non-PKI MFAs derived from that PKI credential must be immediately revoked.

[17] This section replaces Section 3.5.d of DoDI 8520.03.

[18] Where this is not technically feasible (e.g., the expiration date for a hardware OTP token is hardcoded into the seed file and will be either 3 or 5 years from the date of manufacture), require the user to annually re-register their non-PKI MFA with the user accounts which use the non-PKI MFA.

B. Authentication Strength Requirements

1) **AAL Requirements**: Except for certain approved use-cases in Attachment 4, NIST SP 800-63A Authenticator Assurance Level (AAL) 2 is the minimum required for privileged and non-privileged users (i.e., general users) accessing non-public DoD information. CSPs should decide between requiring NIST SP 800-63 AAL2 or AAL3 DoD-approved non-PKI MFAs as part of an MFA solution based on:
   a) their assessment of the use-case,
   b) the sensitivity of the information being accessed,
   c) the cloud impact level of the cloud environment (if applicable),
   d) the RMF baseline of the system, and
   e) the degree of hardship for the user-base to meet AAL-3 requirements or for the system to support AAL-3 credentials.

2) **Password Requirements:** When using username and passwords as one authentication factor in a DoD-approved non-PKI MFA solution, or by itself as a single-factor authenticator in the few use-cases where this is permitted, CSPs MUST ensure the passwords comply with all the requirements in Section 3.5.a.(3) of DoDI 8520.03. Even if a system owner has enabled PKI or non-PKI MFA for user-authentication, if the password field is still present for an account, the system owner must ensure it complies with section 3.5.a.(3) of DoDI 8520.03.

3) **Passkeys & Passkey-like Technologies:** Passkeys are a type of non-PKI MFA. In addition to this attachment's other requirements, CSPs must ensure the following for passkeys and passkey-like technologies:
   a) Abide by the non-exportability requirements in section 3.2.13 of NIST SP 800-63B.
   b) Securely store, manage, and bind non-PKI MFA passkeys to either a crypto module/engine on a device physically separate from the device being used to authenticate (e.g., USB), or a separate embedded hardware Trusted Platform Module (TPM). This must include physical or logical security mechanisms to prevent exporting the keys outside the device, prevent tampering with the module, and to provide tamper evidence & detection.
   c) Verify with the passkey vendor that the product either doesn't have a key-syncing/sharing capability or that this capability can and will be turned off.
   d) Ensure any settings allowing key-syncing or sharing are turned off by administrators with two-person verification and are checked monthly to ensure they remain off.
   e) Monitor for device reconfigurations or updates that allow key-syncing/sharing with other users or uploads of keys to a cloud provider.
   f) Require all users issued passkeys to sign an agreement to not share their passkeys. Users must only be provisioned device-bound passkeys, and these must only be provisioned on devices for which they are the sole user.
   g) Prevent server-side storage and processing of passkeys.
   h) Ensure DoD relying parties (RP) can verify during registration and, if possible, during all subsequent authentications that passkeys presented for authentication are device bound.
   i) DoD PKI authentication may be used to enroll or change authentication methods for a device-bound passkey.
   j) If the device is not managed by DoD, the RP must wait for a response from the authenticator the user is attempting to register, inspect it to see if the properties of the credential are compliant, and accept or reject the credential accordingly. The best way to differentiate

between a device-bound passkey and a syncable passkey is to inspect the "backup eligible" flag in the authenticator data response. If it is eligible for backup, then it is syncable and not approved for use on DoD systems.[19] Other methods may exist as well.

C. Access Management Requirements

Access management is a vital part of ICAM and can serve as a potential compensating control for weaker authenticators. Access management must be implemented in accordance with DoDI 8520.04, "Access Management for DoD Information Systems." Attachment 4 will address access management for specific non-PKI MFA use-cases. In the event of a conflict between access management requirements in DoDI 8520.04 and Attachment 4 of this document, follow Attachment 4 to the extent necessary to accommodate the use-case and follow 8520.04 for everything else.

[19] For more information, see World Wide Web Consortium (https://w3c.github.io/webauthn/#backupeligibility)

Attachment 4: DoD-Approved non-PKI MFA Use-Cases

The requirements detailed in this attachment supplement the implementation guidance provided in Attachment 3 for specific DoD-approved non-PKI MFA use cases. Attachment 3 requirements remain applicable unless the requirements for a specific use-case say otherwise. These use-cases replace the use-cases in section 3.3 of DoDI 8520.03. This list of use-cases is expected to be a living document. Non-PKI MFA use-cases and implementation requirements may be changed or added to this list as approved by the DoD CIO. The use-cases will be posted and updated at: https://intelshare.intelink.gov/sites/dodcioicamdocs.

Contents

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders) 17

Citizen or Business to Government 17

DoD Beneficiaries, Retirees, and Family Members 17

Recruit 17

Schoolhouse Environment for pre-K-12 Students 18

Schoolhouse Environment for Adult Staff or Adult Students 18

Training Environments 19

Restricted Identity & non-attribution 20

Security Clearance Investigations 20

National Emergency in a US State or Territory 20

Disaster Relief in a US State or Territory 21

Foreign Nationals 22

Foreign Ownership, Control, or Influence (FOCI) Business to Government 23

Guest User Accounts 23

TABLE 2 Users on Unclassified DoD Networks with DoD-approved PKI Credentials (e.g., CAC Holders) 24

Medical Devices & Systems 24

Authentication to DoD GFE Mobile Endpoints (e.g., Devices) 25

Authentication From a Personal Mobile Device (i.e., Bring Your Own Device (BYOD)) 25

TABLE 3 Users on Unclassified DoD Networks and the DoD Secret Fabric with DoD-approved PKI Credentials (e.g., CAC Holders, SIPR PKI Token Holders) 28

Standalone Systems and Closed Restricted Networks 28

Isolated DoD Development, Labs, Ranges, or Test Environments 28

Operationally Constrained Environment/DDIL/ CDOL (e.g., Weapons IT) 29

TABLE 4 IT Privileged Users on Unclassified Networks and the DoD Secret Fabric 30

General IT Privileged User Accounts 30
Legacy System 31
IT Device, Endpoint, or Legacy System Local Logon Accounts 31
Administrator Emergency Accounts for Crisis Situations (i.e., Account of Last Resort) 32

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Citizen or Business to Government	An individual such as a US citizen requires authentication to submit a civilian job application or register for a conference. A US business requires authentication to register to receive requests for proposal or to submit proposals.	For individual, IAL-1 identity-proofing is permitted, but discouraged. If possible, individuals must be provided the option of IAL-2 identity-proofing (e.g., via myAuth). For businesses, a Government Contracting Authority will validate identity and sponsor a user account to receive RFPs or to submit proposals. Post contract award, the company must obtain DoD-approved PKI for continued access.	**Recommended Credentials:** - DoD-approved non-PKI MFAs. **Alternative Credentials:** If user does not have a smart phone, allow phone, e-mail, or text-based one-time passwords (OTP).	User is restricted to access IL2 low-risk information, and user's own low risk PII[20].
DoD Beneficiaries, Retirees, and Family Members[21]	A DoD beneficiary, retiree or family member who has an identity in DMDC's person data repository (PDR) seeking access to DoD systems for health, benefits, education, morale/welfare purposes, or permanent change of station data. This includes designated surrogates acting on behalf of a DoD beneficiary.	If a beneficiary cannot perform IAL-2 documentation-based identity-proofing, they may perform other types of identity-proofing provided they comply with all other IAL-2 requirements in NIST SP 800-63A.[22]	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** If user does not have a smart phone, allow phone, e-mail, or text-based OTP.	User is restricted to access IL2 low-risk information, and user's own PII and PHI.
Recruit	Pre-accession recruits seeking access to resources related to their own record. These users have not been registered in the DoD PDR and not been issued a CAC.	For the initial intake of a potential recruit, IAL-1 is acceptable. Once a recruit demonstrates intent to continue through the recruitment process, the recruiter must transition	**Recommended Credentials**: - DoD-approved non-PKI MFAs **Alternative Credentials**: For initial intake, allow phone, e-mail or text-based OTPs.	Until the recruit is issued a DoD-approved non-PKI MFA, restrict the recruit's access: - to only IL2 low-risk information, and to the user's own low risk PII.

[20] Low Privacy Risk PII is a small subset of PII. For additional information, see the NIST RMF Privacy Overlay in CNSSI 1253F, Attachment 6, at https://www.cnss.gov/CNSS/issuances/Instructions.cfm. Also see the RMF Knowledge Service at https://rmfks.osd.mil/rmf/RMFforDoDTech/Pages/PrivacyRoleinRMF.aspx.

[21] This use-case also applies to a DoD CAC-holder using a non-DoD workstation or device to access this type of non-mission data.

[22] Note: While Knowledge-Based Verification (KBV) is forbidden by NIST SP 800-63A, beneficiaries may continue using it with DS-Logon (DSL) until the end of 2025.

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
		the recruit to at least IAL-2 documentation-based identity proofing and comply with the other credential lifecycle requirements (i.e., credential issuance, credential maintenance and revocation) in Attachment 3.	Once a recruit demonstrates intent to continue through the recruitment process, issue them a DoD-approved non-PKI MFA and revoke other MFA. Once a recruit is issued a CAC, revoke the DoD-approved non-PKI MFA unless it's needed for another approved use-case.	- at the recruitment resource/endpoint to information that has been authorized for release to untrusted users or devices
Schoolhouse Environment for pre-K-12 Students	This use case is limited to non-DoDIN educational environments for preschool, elementary, middle, and high school students with .edu domains that have no direct network connectivity to any other DoD resources or networks. These environments may leverage commercial cloud services, ensuring these educational institutions can operate independently of the DoD. For example, a DoDEA student accessing a DoDEA system from home or on the DoDEA network for school curricula, lessons, homework, and tests.	IAL-1 identity-proofing and third-party identity-proofing are both acceptable for pre-school, elementary, middle, and high school students at a DoDEA or similar DoD-run school, provided the student has DoD Sponsorship, or Command Sponsorship for overseas locations. If the student has been issued a DoD ID (formerly referred to as the EDIPI), the DoD ID must be validated as well.	**Recommended Credentials**: - DoD-approved non-PKI MFAs **Alternative Credentials**: Students may use username and password to authenticate to their accounts and information, but MFA should be used whenever possible. AOs may waive the password implementation requirements from Section 3.5.a.(3) of DoDI 8520.03 for students deemed too young to comply with them.	Student must be blocked from accessing non-.edu DoD networks, systems, or websites. Students must be restricted to accessing only their own accounts and education-related materials on the .edu network and internet.
Schoolhouse Environment for Adult Staff or Adult Students	Staff members and Adult Students of DoD Educational Institutions hosted in a .edu environment who are NOT eligible for DoD-approved PKI (e.g., substitute teachers,	Use at least IAL-2 documentation-based Identity-proofing. Comply with other credential lifecycle requirements in Attachment 3.	**Recommended Credentials**: - DoD-approved non-PKI MFAs **Alternative Credentials**: If user does not have a smart phone,	These users must be restricted in their access to PII, and appropriate measures must be implemented to prevent PII disclosure.

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
	cafeteria workers, foreign national students)		allow phone, e-mail or text-based OTPs.	These users must be blocked from accessing non-.edu DoD networks from their school networks and devices, including the NIPRNet. No direct network connections are permitted.[23] If there is a need to grant these users access to a public-facing DoD website with a DoD-approved non-PKI MFA, their access must be tightly restricted to information needed to perform their duties.
Training Environments	A DoD, federal, or industry partner employee or user (e.g., contractor) who is required to complete recurring DoD security training or other DoD mandated training or need access to their DoD training records. These users either don't have DoD-approved PKI or don't have DoD network accounts. Examples would include: 1) A DoD user who needs to complete their annual security training to obtain or renew their network account. 2) A small business without resources for ECAs that needs access to recurring DoD	Use at least IAL-2 documentation-based Identity-proofing. Comply with other credential lifecycle requirements in Attachment 3.	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** If user does not have a smart phone, allow phone, e-mail or text-based OTPs.	The user must be restricted to access CUI (IL4) low-risk non-mission critical training environments and information

[23] Please note this is not intended to restrict DoDEA employee access to DoD networks and network resources from GFE using DoD-approved PKI credentials.

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
	security training to do business with DoD.			
Restricted Identity & non-attribution	Non-DoD federal students and other DoD or intelligence personnel requiring security-related training without attribution to assigned agency.	Administrators of the system in question or a trusted proxy (e.g., intel agency) will identity-proof users via IAL-2 documentation-based identity-proofing described in Attachment 3. The information may be stored in a dedicated system and not shared with the rest of DoD. The AO may waive credential lifecycle requirements in Attachment 3 if they deem it necessary to protect the user's identity.	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** If user does not have a smart phone, allow phone, e-mail, or text-based one-time passwords (OTP).	User restricted access through public facing web application to necessary training materials.
Security Clearance Investigations	A user needs access to a DoD system to fill in their personal SF-8X information as part of their initial clearance investigation or re-investigation.	Investigator will identity proof users via IAL2 documentation-based identity-proofing described in Attachment 3 before registering them with the D-ICAM system. Comply with other credential lifecycle requirements in Attachment 3.	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** If user does not have a smart phone, allow phone, e-mail or text-based OTPs.	User is restricted to access IL2 low-risk information, and user's own PII and PHI, including their SSN, for their own account. The system used for this function must implement NIST SP 800-53 Security Controls, including privacy overlays. The system architecture must not be a relational database. The AO must authorize the system IAW DoDI 8510.01 Risk Management Framework and determines what files are saved in the system.
National Emergency in	Immediate aftermath of a man-made or national disaster, such	If a DoD Component does not have the on-site resources for credential or	**Recommended Credentials:** - DoD-approved non-PKI MFAs	Limit access at the disaster-response resource/endpoint to

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
a US State or Territory	as an attack, large-scale civil unrest, mass evacuation, severe infrastructure failures, chemical/radiological incidents, where the Local Commanding Officer (LCO) is operating under Immediate Response Authority and needs to grant rapid access to unclassified DoD information resources to non-DoD personnel.	documentation-based identity proofing, they may use third-party identity-proofing. The LCO may waive third-party identity-proofing if they are willing to accept the risk. The LCO may also waive other credential lifecycle requirements if they are willing to accept the risk (i.e., credential issuance, credential maintenance and revocation).	**Alternative Credentials:** - If the emergency precludes obtaining and using a DoD-approved non-PKI MFA, the LCO may authorize non-approved non-PKI MFAs such as phone, e-mail, or text-based OTP for the duration of the emergency. - If the emergency precludes use of any MFAs, the LCO may authorize username and password. - If the emergency precludes compliance with the password requirements in section 3.5.a.(3) of DoDI 8520.03, the LCO may waive these requirements.	information that has been authorized for release as part of the disaster response. If possible, set up an online portal for sharing DoD information that is separate from DoD networks and systems.
Disaster Relief in a US State or Territory	Serious disruption of the functioning of a community causing widespread human, material, economic, or environmental losses that exceed the affected community's ability to cope using its own resources; likely resulting in first responders, emergency services, federal partners, and NGOs needing limited logical access to DoD information resources to manage the disaster and save lives (e.g., Defense Support of Civil Authorities).	If a DoD Component does not have the on-site resources for credential or documentation-based identity proofing, they may use third-party identity-proofing.	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** - If the emergency precludes obtaining and using a DoD-approved non-PKI MFA, the LCO may authorize non-approved non-PKI MFAs such as phone, e-mail, or text-based OTP until DoD-approved non-PKI MFAs can be supported.	Limit access at the disaster-response resource/endpoint to information that has been authorized for release as part of the disaster response. If possible, set up an online portal for sharing DoD information that is separate from DoD networks and systems.

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Foreign Nationals[24]	Foreign nationals (FN) who support foreign governments and need limited access to specific unclassified DoD systems. Examples include: 1) A CCMD (i.e., COCOM) needs short-term assistance from locals on a project. 2) A CCMD owns and runs an information system specifically intended to rapidly engage foreign mission partners in nontraditional missions such as humanitarian assistance, disaster response, or stability operations. 3) Foreign users from many different countries need limited access to a small number of public-facing DoD websites for training, exercises, or Foreign Military Sales (FMS).	If a DoD Component does not have the infrastructure or on-site resources for credential or documentation-based identity proofing, they may use third-party vouching.	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** If the foreign user does not have a smart phone, require them to use land line phone, e-mail or text-based OTPs in combination with a username and password.	Limit FN access in accordance with applicable DoD policies.[25] Block FNs from administrative or unrestricted roaming access within the system environment. Limit FN access at the resource/endpoint, and isolate FN access to assigned lines of effort. Implement security groups, web-app firewalls, and network segmentation as necessary to enforce these rules. An FN from one country should not be able to view information from another country, or which the US has given to another country, unless they have a mission need AND the US and the second country grant permission. If possible, use an online portal separate from other DoD networks and systems to host the DoD information for FNs.

[24] Note: This use-case does not apply to FNs who need network level access to unclassified DoD networks and/or broad access to CUI across multiple DoD systems as part of their day-to-day office duties. These FN users must obtain DoD-approved PKIs in accordance with DoDI 8520.02. This use-case also does not apply to "embedded" foreign nationals, who are subject to the requirements in DoDD 5230.11, DoDD 5230.20, and other pertinent DoD policies.

[25] For FN access to CUI, see DoDI 5200.48 and OUSD(I&S) Memorandum "Change to Policy on Sharing CUI with Foreign Entities," January 31, 2024.

TABLE 1 Users on Unclassified DoD Networks Without DoD-approved PKI Credentials (e.g., Non-CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Foreign Ownership, Control, or Influence (FOCI) Business to Government	Vendors are required to submit a SF-328 FOCI package when bidding on a gov't contract valued more than $5 million. This is a pre-award of contract, and the gov't cannot legally require the company to acquire a DoD External Certificate Authority (ECA) PKI or other DoD-approved PKI at this point.	Gov't Contracting Authority will validate individual's identity and sponsor user account to complete the FOCI SF-328 submission. Post contract award, company must obtain DoD-approved PKI for continued access.	**Recommended Credentials:** - DoD-approved non-PKI MFAs **Alternative Credentials:** Allow phone, e-mail, or text-based one-time passwords (OTP) if user does not have a smart phone.	SF-328 FOCI packages contain proprietary company CUI and must be protected in accordance with DoD CUI policy. The submission is through a public-facing web application, but the submitted info must be stored in an IL5/ RMF High Confidentiality environment. Users must only have access to their own company's submissions and be blocked from accessing other companies' data.
Guest User Accounts	Some DoD Components allow their employees to sponsor non-DoD users for guest-user accounts on certain systems.	The DoD Component must: - Draft a policy on who may grant and be granted guest user accounts. - Run a basic criminal background check on all sponsored guest users. - Require sponsors to sign an agreement accepting responsibility for the guest user, including revocation of credentials or accounts if the guest's MFA is lost, stolen, or compromised. - Require sponsored guest users to report lost, stolen, or compromised credentials within 24 hours. - Require periodic reauthorization of sponsored guest accounts.	**Recommended Credentials:** - DoD-approved non-PKI MFAs. **Alternative Credentials:** None.	Permit access up to IL4/RMF Moderate Confidentiality information, provided guest user is appropriately sponsored, vetted, and trained. No access to CUI. No access to PII unless it is low risk PII.

TABLE 2 Users on Unclassified DoD Networks with DoD-approved PKI Credentials (e.g., CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Medical Devices & Systems	Special purpose systems or devices used for diagnostic or interventional care at DoD-affiliated Medical Treatment Facilities (MTF). Either they can't support DoD-approved PKI or non-PKI MFA credentials, or there are concerns the credentials could interfere with medical operations, limit the utility of the medical device in an emergency, and/or violate FDA regulations for bringing outside items into an MTF.	No change from Attachment 3.	**Recommended Credential:** Imprivata iAccess Tap & Go cards with a PIN. AOs may waive the FIPS-140, NIAP PP, and phishing-resistance requirements in the authentication strength section of Attachment 2. Clinicians may maintain an active login with multiple simultaneous sessions and screens for the medical devices. For a typical workstation, they must use DoD-approved PKI (e.g., CAC) unless forbidden to bring their PKI tokens into the MTF. **Alternative Credentials:** If a medical device account cannot support any PKI or non-PKI MFA, and there is an urgent need for its use, the AO may permit username & password. If a password proves necessary for administrator accounts, it may not be the same administrator password used on other devices in the facility.	Limit DISN connections to infrastructure services (e.g., Active Directory, Host Based Security System, patching). Otherwise, logically isolate from DISN. Lock DoDn the medical device or system from Internet browsing or e-mail and restrict access to controllers or workstations which are also locked DoDn. Place the device or system in a controlled environment with physical security. Assign the device or system to a medical device enclave that is compliant with the Medical Device Security Technical Implementation Guidance (STIG). The enclave must use an isolated virtual Local Area Network (VLAN) configuration with defined routing through isolated subnets. Restrict user access to the underlying OS of the device or system. Only allow the use of Imprivata iAccess Tap & Go cards in facilities that do not allow DoD-approved PKI to brought in from outside the facility or for medical devices that either can't support DoD-approved PKI or non-PKI MFA credentials or for which there are concerns that DoD-approved PKI or non-

TABLE 2 Users on Unclassified DoD Networks with DoD-approved PKI Credentials (e.g., CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
				PKI MFA credentials could interfere with medical operations or limit the utility of the medical device in an emergency. The Imprivata cards may not leave the MTF where they are designated for use.
Authentication to DoD GFE Mobile Endpoints (e.g., Devices)	Unlocking (i.e., gaining access to) a DoD GFE mobile device. [Authentication FROM the DoD GFE Mobile Device to DoD functions, applications, systems, cloud environments, or networks should be done with DoD Mobile PKI credentials (e.g., Purebred PKI certificates stored on the device or on FIPS-approved Yubikeys) in accordance with the DoD CIO memorandum "DoD Mobile Public Key Infrastructure (PKI) Credentials," December 20, 2019."]	The GFE mobile device must be issued in line with DoD Component processes.	Single-factor authentication (e.g., PIN or password) may be used to unlock the device ONLY. The specific method for unlocking the device will be chosen and implemented in accordance with applicable DISA STIGs. Use of the device to authenticate to DoD functions, applications, systems, cloud environments, or networks should be with DoD-approved Mobile PKI credentials.	Access to the device must be restricted in accordance with applicable DoD policies and DISA STIGs. The device must be protected in accordance with applicable DoD policies and DISA STIGs.
Authentication From a Personal	Users authenticating with DoD approved non-PKI MFAs to DoD	The DoD-approved non-PKI MFA must be derived from the user's	**Recommended Credentials:** - DoD-approved non-PKI MFAs.	Block user access to IT Privileged User Accounts, regardless of whether the device is using a MAM or VDI.

TABLE 2 Users on Unclassified DoD Networks with DoD-approved PKI Credentials (e.g., CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Mobile Device (i.e., Bring Your Own Device (BYOD))	environments or data via personal mobile device, using either a Mobile Application Management (MAM) implementation or a Virtual Desktop Interface (VDI).	DoD-approved PKI in accordance with the "Identity-proofing for Users Who Have a DoD-approved PKI Credential" section of Attachment 3.	**Alternative Credentials:** Purebred PKI certificates are currently only issued to GFE mobile devices. Should Purebred PKI certs become approved and available for personal devices, DoD Components must plan for transitioning the personal devices away from non-PKI MFA to Purebred PKI. **Device Management:** - Comply with the following DoD Guidance: • "Use of Non-Government Owned Mobile Devices," August 10, 2022. • "Use of Unclassified Mobile Applications in Department of Defense," October 6, 2023. • "Supplemental Guidance to the Federated Implementation of Office Collaboration Capabilities for the DoD", November 25, 2020. • "Follow-on Supplemental Guidance to the Federated Implementation of Office Collaboration Capabilities for the DoD – Direct Access", January 11, 2021. • DISA Memorandum "M365 DoD, Cross-Tenant Collaboration Tenant Configuration Guide (TCG)", March 26, 2021. • NIAP Mobile Device Fundamentals Protection Profile and DoD Annex. Ensure the device and any DoD-managed applications on the device have anti-tamper	Users may access M365 applications and services hosting data up to (and including) CUI, regardless of whether the overall Cloud Impact Level (IL) of the M365 cloud environment hosting the M365 application or service is IL2, IL4, or IL5. Implement data-tagging and conditional access control. If technologically feasible, configure a Virtual Machine (VM) or some other type of sandbox to help isolate the user's DoD-related activities from other parts of the personal device. If the user is accessing a DoD application on the device, ensure the application is managed and isolated from the rest of the device to the extent possible. Utilize Risk Based Conditional Access or a similar method to ensure only authorized applications and services are being accessed from the MAM or VDI. For MAM, limit access to applications that can be policy enforced. Utilize Risk-based Access evaluation to monitor current authentication and authorization sessions. If the risk level increases for the authentication session, the application session or overall cyber posture of the

TABLE 2 Users on Unclassified DoD Networks with DoD-approved PKI Credentials (e.g., CAC Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
			mechanisms built in. These features should activate if the phone detects a security risk (e.g., tampering) or if the user has not logged into their account for a certain period. Ensure DoD Devices enrolled with device bound passkey can be automatically removed from enrollment in response to changes in risk for the authentication session, the application session, or overall cyber posture of the environment. Prevent server-side storage and processing of passkeys and biometric data. Biometrics must be maintained as a local match only on a device or authenticator that the user controls.	environment, system and domain administrators must be able to revoke the current authentication and session tokens. Personal devices/BYOAD may not be used to access the DoD Secret Fabric or any other classified networks or systems.

TABLE 3 **Users on Unclassified DoD Networks and the DoD Secret Fabric with DoD-approved PKI Credentials (e.g., CAC Holders, SIPR PKI Token Holders)**				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Standalone Systems and Closed Restricted Networks	Standalone Systems and Closed Restricted Networks where access to live operational systems and networks is blocked (e.g., the systems within the CRN have no DISN or commercial internet access but the network backbones do with appropriate security configurations).	The DoD-approved non-PKI MFA should be derived from the user's DoD-approved PKI in accordance with the "Identity-proofing for Users Who Have a DoD-approved PKI Credential" section of Attachment 3. If this is not possible due to network connection constraints, the user must at a minimum demonstrate they are in possession of a DoD-approved PKI at medium-hardware assurance or above at the time of provisioning (and periodically thereafter).	**Recommended Credentials:** - DoD-approved PKI with CRL/OCSP limitations when the network or system can support it. **Alternative Credentials:** DoD-approved non-PKI MFAs (see Attachment 2 for Secret Fabric restrictions on non-PKI MFAs). On unclassified networks only, if the network or system can't support any DoD-approved PKI or any DoD-approved non-PKI MFA, the AO may authorize phone, e-mail, or text-based one-time passwords (OTP). AOs may only authorize username & password (UN/PW) if no MFAs, including e-mail, phone, or text-based OTP, are operationally feasible.	The user must present a valid unexpired DoD-approved physical access credential (e.g., CAC) to gain physical access to the space (e.g., SCIF) hosting the system or network. The system or network: • Must not have the ability to access a live, operational network. • Cannot transmit, receive, route, or exchange information outside of the system or network boundary (except for patches, updates, or CRLs). • Must reside in physical spaces that have commensurate physical controls that restrict access to only authorized users.
Isolated DoD Development, Labs, Ranges, or Test Environments	Information systems that collect or process test data that are either: - not externally connected to live operational networks - have highly controlled connections.	No change from Attachment 3.	**Recommended Credentials:** - DoD-approved non-PKI MFAs (see Attachment 2 for Secret Fabric restrictions on non-PKI MFAs). **Alternative Credentials:** If the environment can't support DoD-approved non-PKI MFA or full compliance with Attachment 2,	The Alternative Credentials in the "Authentication Strength" column for this use-case may not be used in a production environment.

TABLE 3 Users on Unclassified DoD Networks and the DoD Secret Fabric with DoD-approved PKI Credentials (e.g., CAC Holders, SIPR PKI Token Holders)				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
			the AO may authorize a non-approved MFA, or an approved non-PKI MFA that doesn't meet all the authentication strength requirements in Attachment 2, for use in the isolated lab environment only.	
Operationally Constrained Environment/DDIL/ CDOL (e.g., Weapons IT)	DoD users trying to access resources in operationally constrained environments, such as denied, degraded, intermittent, or limited bandwidth (DDIL) environments or Contested, Degraded, and Operationally Limited (CDOL) environments. PKI-based authentication is often constrained by the available network infrastructure or bandwidth (e.g., revocation checking is difficult).	Attachment 3 requirements which are operationally infeasible due to operational constraints may be suspended. These practices must resume when operationally feasible. Information on credential revocation or account disablement should be cached and updated when feasible. If a DoD-approved PKI is revoked because it was lost or stolen, the AO may permit non-PKI MFAs derived from (and therefore linked) to that PKI credential to remain valid for up to 45 days until the user obtains another DoD-approved PKI credential.	**Recommended Credentials:** - DoD-approved PKI (including software PKI if necessary[26]) credentials where operationally feasible. **Alternative Credentials:** DoD-approved non-PKI MFAs where DoD-approved PKI credentials are not operationally feasible (see Attachment 2 for Secret Fabric restrictions on non-PKI MFAs). On unclassified networks only, if the environment can't support any DoD-approved PKI or any DoD-approved non-PKI MFA, the AO may authorize phone, e-mail, or text-based OTP. AOs may only authorize username & password (UN/PW) if no MFAs, including e-mail, phone, or text-based OTP, are operationally feasible.	With UN/PW, text or e-mail OTP, or non-approved MFA, restrict access to IL2/RMF Confidentiality Low where possible. With DoD-approved PKI or DoD-approved non-PKI MFA, allow access up to CUI/IL5/RMF Confidentiality High.

[26] Note that this is one if the very few use-cases where a DoD software PKI certificate may be used for user-authentication (as opposed to a device-authentication).

TABLE 4
IT Privileged Users on Unclassified Networks and the DoD Secret Fabric

Use-Case	Description	Credential Lifecycle	Authentication Strength	Access Management
General IT Privileged User Accounts	Examples of use-cases where IT Privileged Users may need to use non-PKI MFA to authenticate to their IT Privileged User Accounts include, but are not limited to: **1)** Network devices (e.g., routers, switches) which demonstrably do not support PKI (e.g., command line authentication into a network device where the user is connecting through Secure Shell and there's no smart card reader pass through into the environment). **2)** A commercial CSO does not support PKI authentication to the CSO's servers (e.g., for access to CSO management interfaces). **3)** System admins are required to use a non-PKI MFA along with their PKI as an additional layer of	The user must possess a CAC, PIV, or ALT PKI Credential. The DoD-approved non-PKI MFA must be derived from the user's DoD-approved PKI in accordance with the "Identity-proofing for Users Who Have a DoD-approved PKI Credential" section of Attachment 3.	**Recommended Credentials:** - RSA HW SecurID Tokens. - YubiKey with FIDO2 Passkey. - SafeNet 110 OTP HW Token. **Alternative Credentials (unclassified networks only):** - Army/AF MobileConnect. - MS Auth with Passkey. - Okta Verify with FastPass. (NOTE: For IT Privileged User Accounts, these authenticators must be stored on a separate device from the device being used to authenticate to DoD resources. For example, the user authenticates to the IT Privileged Account from a DoD GFE device, but the authenticator is stored on a TPM on a separate personal device). For both recommended and alternative credentials, the user **must** first authenticate with DoD-approved PKI to a DoD network, VPN, or CITRIX **before** using the DoD-approved non-PKI MFA to access their IT Privileged User account. Non-PKI MFAs, regardless of whether they're DoD-approved, **must not** be used for initial authentication to DoD networks, VPN, or CITRIX to access IT Privileged User Accounts.	Implement DoD-approved Privileged Access Management (PAM) Tools consistent with DoD Policy. Block authentication to IT privileged user accounts from non-US government owned or managed devices unless the authentication is through DoD VPN or DoD Citrix. This includes blocking authentication to privileged virtual profiles from personal devices. Use an out-of-band network for privileged-user authentication. Ensure access to the devices or server administrative accounts is tightly controlled. Implement separation of duties and least privileged access. Constrain privileged user access to specific workstations or virtual desktop profiles expressly approved and configured on a per-environment basis. Ensure privileged users leveraging a GFE workstations do not use the same profile for administrative functions as their general user profile. A separate authenticator bound to the administrator profile must be used to access GFE workstations. For virtual desktops, a separate privileged profile must be leveraged that is bound to the administrator authenticator such that the user may not access privileged functions

TABLE 4 IT Privileged Users on Unclassified Networks and the DoD Secret Fabric				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
	security for accessing their admin consoles.			while logged in via their non-administrator authenticator. Comply with the applicable requirements in Technical Attachment 1 to CYBERCOM TASKORD 14-0018.
Legacy System[27]	Legacy information system can't support PKI or non-PKI MFA. The system owner puts a DoD-approved Identity Federation Service (IFS) (e.g., F5 server), Identity Provider (IdP) or PAM tool in front of the system to facilitate authentication at the front-end until the legacy system can be a replaced with a new system which can handle stronger authentication (which should be done as soon as feasible).	If the IFS, IdP, or PAM tool can't support PKI authentication at the front end, use a derived DoD-approved non-PKI MFA that complies with the "Identity-proofing for Users Who Have a DoD-approved PKI Credential" section of Attachment 3.	**Recommended Credentials:** If the IFS, IdP, or tool can support PKI authentication at the front end, use DoD-approved PKI. **Alternative Credentials:** If the IFS, IdP, or tool cannot support PKI authentication at the front end, use one of the following DoD-approved non-PKI MFAs for authentication at the front-end to access IT Privileged User Accounts: - RSA HW SecurID Tokens. - YubiKey with FIDO2 Passkey. - SafeNet 110 OTP HW Token.	Utilize commercial best practices for access management. If an IFS (e.g., F5 server) or an IdP is used, comply with the IdP requirements in Section 3.6 of DoDI 8520.03. Authentication or assertions from the F5, IdP, or PAM to the legacy system on the back-end should be as secure as possible. If a PAM tool is used, utilize ephemeral passwords on the back-end.
IT Device, Endpoint, or	Local administrator logon to an IT device or endpoint, when network access or	DoD-approved non-PKI MFAs must be derived from the user's	**Recommended Credentials:**	IF UN/PW is used, these accounts must:

[27] This use-case also applies to unprivileged users with DoD-approved PKI (e.g., CAC holders). The unprivileged users may use other approved non-PKI MFAs for unprivileged accounts.

TABLE 4 IT Privileged Users on Unclassified Networks and the DoD Secret Fabric				
Use-Case	**Description**	**Credential Lifecycle**	**Authentication Strength**	**Access Management**
Legacy System Local Logon Accounts	normal logon is unavailable. For example, an administrator may need to logon to a legacy system which can't support PKI or MFA to set up an F5 server in front of it for access by unprivileged users.	DoD-approved PKI in accordance with the "Identity-proofing for Users Who Have a DoD-approved PKI Credential" section of Attachment 3.	- DoD-approved non-PKI MFAs (see Attachment 2 for Secret Fabric credential restrictions). **Alternative Credentials:** UN/PW IF all the requirements under access management are met. Passwords must be: • In compliance with Section 3.5.(3) of DoDI 8520.03.	• Not be used at any other time or for any other purpose. • Be disabled from remote access. • Reside in a physical space that restricts access to authorized users. For endpoint local logon to devices which can't be restricted to a single physical space, the user must have a capability to remotely lock or zeroize the device if the device is no longer under their positive control.
Administrator Emergency Accounts for Crisis Situations (i.e., Account of Last Resort)	Emergency accounts used by IT Privileged Users in response to crisis situations.	The user must possess a CAC, PIV, or ALT PKI Credential. Other Credential Lifecycle requirements may be suspended if necessary.	**Recommended Credentials:** - DoD PKI software certificates[28] - DoD-approved non-PKI MFAs. **Alternative Credentials:** UN/PW may be used for single-factor authentication directly to the server or account. Passwords must be: • In compliance with Section 3.5.(3) of DoDI 8520.03. • Stored in a safe or other locked container, and only removed & used under two-person control. • Deleted and reset after one use.	AOs must ensure these emergency accounts are: • Only accessible in crisis situations when network access or normal logon is unavailable. • Disabled after normal operations resume, & set to automatically disable after a preset amount of time based on the anticipated duration of the situation • Configured to alert administrators when they are being used (alert functionality should be tested periodically during normal operations). • Compliant with applicable DISA STIGs.

[28] Note that this is one if the very few use-cases where a DoD software PKI certificate should be used for user-authentication (as opposed to a device-authentication).