DoD Instruction 8520.04

Access Management for DoD Information Systems

Originating Component: Office of the DoD Chief Information Officer

Effective: September 3, 2024

Releasability: Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.

Approved by: Leslie A. Beavers, Acting DoD Chief Information Officer

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

- Establishes policy, assigns responsibilities, and provides direction for managing access to DoD information technology (IT) resources hosted by systems and system components by person and non-person entities (NPEs) in conformance with DoD Instruction (DoDI) 8500.01.
- Establishes policy and prescribes procedures for systems and system components – including information, control, and weapons systems – that host DoD IT resources.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance 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 United States Coast Guard (USCG) for USCG-operated DoD systems and networks and for USCG systems and networks that directly affect the DoD Information Network (DoDIN) and DoD mission assurance in accordance with the January 17, 2017 Memorandum of Agreement between the Department of Defense and the Department of Homeland Security.

(3) Any digital environment and facility that is used to support access to the digital resources for which DoD or DoD-related data is stored, transited, or processed. At a minimum, this includes **all** networks used to store, transit, or process Unclassified, Secret, Top Secret information, as well as U.S.-owned networks, and all systems under the authority of the Secretary of Defense. These include:

(a) Non-classified Internet Protocol Router Network (NIPRNET).

(b) SECRET Internet Protocol Router Network (SIPRNET).

(c) Joint Worldwide Intelligence Communication System (JWICS).

(d) Defense Research and Engineering networks.

(e) NIPRNET and SIPRNET de-militarized zones.

(f) DoD Mission Partner Environment. Federated access requirements for mission partners in the DoD Mission Partner Environment will be included in a future document.

(g) Contractor networks and systems under the National Industrial Security Program.

(h) Systems hosted on the DoDIN.

(i) Systems hosted at DoD data centers.

(j) Systems in closed operational networks with no connection to the Defense Information Systems Network.

(4) DoD Components responsible for systems that are owned and operated by or on behalf of the DoD, including those identified in Paragraph 1.1.a.(3) as well as:

(a) Control systems.

(b) Systems operated by contractors or other external mission partners that process DoD-owned information.

(c) Commercial cloud services that host DoD IT resources.

(5) Any digital environment and facility that is used to support access to the digital resources for which DoD or DoD related data is stored, transited, or processed. At a minimum, this includes DoD Components granting access to all DoD and non-DoD entities including person entities and NPEs accessing DoD Unclassified, Secret, or Top Secret networks and systems under the authority of the Secretary of Defense, including external mission partners and DoD beneficiaries.

b. This issuance does **not** apply to:

(1) Systems processing, storing, or transmitting special access programs pertaining to intelligence sources, methods, and activities (but not including military operational, strategic, and tactical programs) under the existing authorities and policies of the Director of National Intelligence in accordance with Executive Order 13526.

(2) Systems operated by the DoD Special Access Program (SAP) community. Due to the highly sensitive nature of SAPs and their materials, these systems must be managed independently and fall under the purview of the DoD Chief Information Officer (CIO). For additional details regarding SAP requirements, please contact the Office of the DoD CIO (SAP).

(3) Systems processing, storing, or transmitting Restricted Data and Formerly Restricted Data. The handling of Restricted Data and Formerly Restricted Data within DoD is controlled jointly under the existing authorities and policies of the Secretary of Energy and the Deputy Assistant Secretary of Defense for Nuclear Matters pursuant to Division A of Chapter 23 of Title 42, United States Code, also known as the “Atomic Energy Act, as implemented through Part 1045 of Title 10, United States Code of Federal Regulations”.

(4) Systems in closed non-operational research, development, testing, and evaluation enclaves.

1.2. POLICY.

Access to DoD information systems will be managed to preserve DoD security. While DoD information systems should be as efficient and interoperable as possible, IT resource and system owners must follow the protocols in Section 3 and the procedures in this issuance for access management.

SECTION 2: RESPONSIBILITIES

2.1. DOD CIO.

In addition to the responsibilities in Paragraph 2.9., the DoD CIO:

a. Provides guidance to facilitate the implementation of access management processes and procedures, including maintaining the "DoD Identity, Credential, and Access Management (ICAM) Reference Design."

b. Coordinates with ICAM Executive Board (formerly called the Identity Protection and Management Senior Coordinating Group) members, OSD Component heads, the DoD Component heads, and the Director, ICAM Joint Program Integration Office to prioritize requirements and oversee enterprise ICAM services that support access management activities, including dynamic access.

c. Coordinates with the OSD Component heads and DoD Component heads to develop and maintain requirements for DoD ICAM solutions, including federation of DoD Component-level ICAM solutions with DoD enterprise ICAM services.

d. Develops and maintains requirements and associated standards for the definition, collection, verification, maintenance, protection, and publication of attributes used to support access, including attribute federation with external mission partners.

e. Approves DoD enterprise authoritative attribute services as described in Section 5.

f. Maintains a list of approved DoD enterprise authoritative attribute services in a format that is accessible to system owners.

g. Coordinates with the Chief Data and Artificial Intelligence Officer (CDAO), other OSD Component heads, and DoD Component heads to monitor migration to dynamic access to meet mission needs and identify any changes needed during the migration.

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 2.9., the Director, DISA:

a. Establishes, operates, tests, and maintains DoD enterprise ICAM services that support access management activities.

b. Provides cybersecurity services for DISA-operated enterprise ICAM services in accordance with DoDI 8530.01.

c. Establishes, operates, tests, and maintains enterprise ICAM services managing NPE attributes.

d. Coordinates with the Director, National Security Agency/Chief, Central Security Service to develop, update, and maintain security requirements guides and security technical implementation guides for products and services that support access management, incorporating National Information Assurance Partnership validation where applicable.

e. Provides subject matter expertise and technical support to the DoD Components for:

(1) Implementation of access management capabilities.

(2) Interoperability, data sharing, and integration with DoD enterprise ICAM services operated by DISA to support access control.

2.3. CDAO.

In addition to the responsibilities in Paragraph 2.9., the CDAO:

a. Establishes DoD-level data tagging standards to be implemented across the DoD.

b. Develops policy that incorporates requirements for tagging data, data sets, and digital resources to support dynamic access into data policies and standards.

c. Establishes guidelines for the implementation of digital policy to support dynamic access decisions.

d. Develops DoD enterprise digital policy to support dynamic access in accordance with applicable laws, policies, and other regulations such as DoDI 5200.48 and DoD Manual (DoDM) 5200.01.

e. Develops a governance framework and standards for development, delivery, and adoption of digital services and data, analytics, and artificial intelligence (AI) capabilities.

f. Establishes and chairs the CDAO Council to oversee and resolve issues related to the adoption and use of digital services and data, analytics, and AI capabilities. Communicates and coordinates with other governance forums and officials, including those in the Intelligence Community, as needed to address shared equities or potential conflicts.

g. Selectively scales proven digital services, data, analytics, and AI-enabled solutions, for enterprise and joint use cases in coordination with decision-makers at all levels of the DoD.

2.4. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

In addition to the responsibilities in Paragraph 2.9., the USD(I&S):

a. In accordance with DoDD 5143.01, coordinates with the DoD CIO and members of the intelligence, counterintelligence*,* counter-insider threat*,* and security enterprises to identify user attributes and values needed to support sharing of intelligence resources on the DoDIN.

b. Establishes DoD physical security requirements and interfaces for physical access to systems, facilities, and IT resources.

c. Establishes information security and operations security policy and procedures for tagging data, data sets, and digital resources to support dynamic access into data policies and standards.

d. In coordination with the CDAO, develops DoD enterprise digital policy rules to support dynamic access in accordance with applicable laws, policies, and other regulations such as DoDI 5200.48 and Volumes 1-3 of DoDM 5200.01.

e. Identifying critical information and indicators requiring operations security countermeasures to deny to unauthorized entities information regarding access to DoD information systems.

2.5. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USD(I&S); the authority, direction, and control exercised by the DoD CIO over the activities of the Cybersecurity Directorate, or any successor organization, of the National Security Agency, funded through the Information System Security Program; and in addition to the responsibilities in Paragraph 2.9., the Director, National Security Agency/Chief, Central Security Service, in coordination with the Deputy CIO for Cybersecurity in their capacity as the DoD Chief Information Security Officer:

a. Coordinates with the Director, DISA to develop and maintain security requirements guides and security technical implementation guides for products and services that support access management, incorporating National Information Assurance Partnership validation where applicable.

b. Supports DoD enterprise ICAM services to address DoD mission requirements through research and development and technical and security guidance to DoD enterprise ICAM service providers.

c. Provides systems engineering support and testing support, including threat assessments, for DoD enterprise ICAM services.

d. Establishes cryptographic requirements and standards for ICAM solutions operating on National Security Systems.

2.6. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)).

In addition to the responsibilities in Paragraph 2.9., the USD(P&R):

a. Serves as the DoD ICAM lead for person entity identities, including maintaining DoD's enterprise person entity identity attribute repository and ICAM person entity identity data management and data distribution services, pursuant to the Office of the DoD CIO's "Department of Defense Identity, Credential, Management and Access (ICAM) Strategy."

b. Establishes policy for the collection, verification, and protection of person entity identity attributes that are centrally managed through DoD's enterprise person entity identity attribute repository.

2.7. DIRECTOR, DEPARTMENT OF DEFENSE HUMAN RESOURCES ACTIVITY.

Under the authority, direction, and control of the USD(P&R), and in addition to the responsibilities in Paragraph 2.9., the Director, Department of Defense Human Resources Activity, through the Director, Defense Manpower Data Center (DMDC):

a. Establishes, operates, tests, and maintains enterprise ICAM services that support management of person entity identity attributes supporting access.

b. Maintains one or more data feed interfaces to provide person entity identity attributes to other DoD enterprise and DoD Component-level ICAM services.

c. Provides cybersecurity services for DMDC-operated enterprise ICAM services in accordance with DoDI 8530.01.

d. Provides subject matter expertise and technical support to DoD Components for integration with DMDC-operated enterprise ICAM services.

2.8. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

In addition to the responsibilities in Paragraph 2.9., the Under Secretary for Research and Engineering will ensure digital rules managing access to DoD scientific and technical information are implemented in accordance with DoDI 5230.24.

2.9. OSD AND DOD COMPONENT HEADS AND THE COMMANDANT, USCG.

The OSD and DoD Component heads and the Commandant, USCG:

a. Establish governance for access management, to include approval processes for attribute services in accordance with standards published by the DoD CIO.

b. Establish policy for access management that addresses requirements identified in this issuance and Zero Trust policies.

c. Coordinate with the DoD CIO, ICAM Executive Board Chair, and the Director, ICAM Joint Program Integration Office to identify and maintain requirements for DoD enterprise ICAM services.

d. Plan, program, and budget to support access management, including integrating DoD enterprise ICAM services as appropriate and federating DoD Components, USCG, and community of interest ICAM services with DoD enterprise ICAM services.

e. Ensure systems owned, operated, or managed by DoD Components and USCG meet access requirements as specified in Section 4.

f. Approve Component- and USCG-level authoritative attribute services.

g. Ensure that DoD Component-, USCG-, and community of interest-level or locally implemented ICAM services that support access management are:

(1) Operated in accordance with this issuance.

(2) Support interoperability and data sharing with DoD enterprise ICAM services.

h. Verify and maintain attribute values for DoD Component and USCG personnel and make attribute values available to DoD enterprise attribute services.

i. Participate in DoD ICAM review boards as required.

j. Provide cybersecurity services for DoD Component- and USCG-operated ICAM services in accordance with DoDI 8530.01.

k. Coordinate with the DoD CIO and CDAO to monitor and improve provisioning and de-provisioning of access or migration to dynamic access to meet mission needs.

2.10. CHAIRMAN OF THE JOINT CHIEFS OF STAFF.

In addition to the responsibilities in Paragraph 2.9., the Chairman of the Joint Chiefs of Staff:

a. Identifies, reviews, and validates authorization requirements used by systems that provide support for joint, allied, and coalition missions.

b. Ensures Combatant Commanders comply with DoD information and personnel security policies regarding:

(1) Access to DoD information and other non-DoD, U.S. information in DoD possession.

(2) Reporting of unauthorized access or disclosures.

c. Coordinates implementation and integration of ICAM services that support access management for non-U.S. external mission partners to comply with this issuance.

SECTION 3: IT RESOURCE AND SYSTEM PROTOCOLS

3.1. IT AND DIGITAL RESOURCE PROTOCOL.

a. IT and digital resource owner is synonymous with the role of information system owner. IT and digital resource owners must implement ICAM access capabilities in accordance with Objectives 2.1. and 2.4. in the Office of the DoD CIO's "DoD Zero Trust Strategy" and the users and data pillars described in their "DoD Zero Trust Reference Architecture."

b. In accordance with IT and digital resource owners, advised by records officers and other compliance professionals, must document authorization requirements for all types of access to the resource in accordance with Section 4. System owners must document authorization requirements for all users in accordance with Paragraph 4.1.b.

c. IT and digital resource owners must define and document IT resources and activities that are subject to logging and monitoring requirements based on resource risk and mission function in accordance with Paragraph 4.4.b.

3.2. SYSTEM PROTOCOL.

a. System owners must implement technical controls to prevent escalation of privileges from access by general users and functional privileged users to IT privileged user access in accordance with an approved enterprise separation of duties (SOD) ruleset.

b. Systems must authenticate users before granting access to any IT resources hosted by the system in accordance with DoDIs 8520.02 and 8520.03.

c. When implementing explicit access, system owners must implement processes to provision and de-provision access based on authorization requirements in accordance with Paragraph 4.2.a.

d. When implementing dynamic access, system owners must only rely on attributes provided by attribute services operated in accordance with Paragraph 4.3.

e. A functional privileged user, also known as an application privileged user, is assigned a specific position or duty within an application, such as approver in a financial management system or a civilian time system. For IT privileged users and functional privileged users, regardless of access method:

(1) Access granted must be based on least privilege, most restrictive access.

(2) System owners must retain traceability between the user and the approval process.

(3) Access and accounts must be traceable to a single user and must not be shared between users. Group accounts, when authorized by an authorizing official, must be traceable to

an assigned sponsor and must be accessed by group alternate logon tokens and documentation of the group membership and usage maintained by the sponsor.

(4) IT privileged users must use separate credentials and separate accounts when accessing the system using elevated privileges to perform IT privileged actions.

(5) System owners must conduct access reviews as described in Paragraph 4.2.a.(5).

f. System owners must limit operating system and application service accounts and the entitlements provisioned to service accounts to those needed to perform required functions.

(1) Access to and use of service accounts and their associated entitlements must be restricted to a specified time and disabled when not in use. National Security Agency-recommended best practices include the use of group managed service accounts, standalone managed service accounts, and workload identities for cloud service accounts.

(2) System owners must regularly review audit logs for these accounts to verify that accounts are still required and are being used only for their intended purpose.

(3) Evidence of access approvals and subsequent reviews must be retained for at least 12 months beyond account deactivation for non-sensitive systems or as required by the business or mission as required by DoDI 8510.01.

(4) Access reviews for all user accounts and entitlements should occur every 12 months when required by the business or mission as required by DoDI 8510.01.

g. System owners must define and document IT resources and activities that are subject to logging and monitoring requirements based on resource risk and mission function in accordance with Paragraph 4.4.b.

SECTION 4: IMPLEMENTATION PROCEDURES

4.1. DEFINING ACCESS REQUIREMENTS.

a. IT Resource Hosting.

(1) IT resources (data, application, etc.) are hosted on IT systems.

(a) The IT resource owner is responsible for:

1. Defining, documenting, and identifying authorization and access requirements for the resource.

2. Providing this information to the IT system owner.

(b) The IT system owner is responsible for implementing and enforcing:

1. Authorization and access requirements provided by the IT resource owner for the IT resources on their system.

2. Applicable information security and operations security policies, including DoDD 5205.02E, DoDIs 5200.02, 5200.46, 5200.48, and 5210.83, and DoDM 5200.01.

(c) IT resource owners and IT system owners should work together to determine the best way to manage access to IT resources on a given system.

(2) Some IT resources may be hosted across multiple systems and some systems may host multiple IT resources. Multiple access policy rules may be needed depending on the requirements of the IT resources. For dynamic access to IT resources hosted by multiple systems, the resource itself should be tagged so that appropriate policy rules can be enforced for access.

b. IT Resource Support.

IT resource owners can support digital policies and data set level access controls by working with the CDAO, USD(I&S), and functional leads to identify and register their data holdings at the data set level.

c. IT Resource Owner Requirements.

IT resource owners, advised by records officers and other compliance professionals, must:

(1) Document authorization requirements for all types of access to the IT resource, considering and applying Zero Trust guidance when completing the requirements. Requirements may be based on laws, regulations, policies, contracts, interagency agreements, international agreements, or other sources. Applicable information security policies and guidance include DoDIs 5200.02, 5200.46, 5200.48, 5210.83, and 8910.01 and Volumes 1-3 of DoDM 5200.01.

(2) Provide documented authorization and access requirements to owners of systems hosting the resource.

(3) Review authorization and access requirements at least annually to confirm that the rationale for such requirements remains appropriate and commensurate with risk.

d. System Owner Requirements.

System owners must document and enforce authorization requirements and methodologies for all users that are aligned with authorization requirements for resources hosted by the system. Requirements must be approved at least annually to confirm that the rationale for such requirements remains appropriate and commensurate with risk. System owners may use explicit access, dynamic access, or a combination as described in Paragraph 4.2., based on the type of user and the capabilities of the system.

(1) Public Access.

Access to IT resources approved for public release in accordance with DoDIs 5230.09 and 5230.29 does not require authentication or authorization.

(2) General Access.

General users must be authenticated in accordance with DoDIs 8520.02 and 8520.03 before being given access to a system or any IT resource not approved for public release.

(a) If the only authorization requirement is maintaining a record of who accessed the IT resource, no additional authorization processes are required.

(b) If access to the IT resource is authorized for an individual (or designee) to whom the resource pertains (e.g., an individual accessing their own information, health record, or training record), the system must verify that the user is the individual (or designee). System owners should use dynamic access to support this verification.

(c) If access to the IT resource is based on verification of specific defined user attributes such as organizational affiliation, completion of a favorable background check, U.S. citizenship, and an active security clearance, the system must implement processes to obtain and verify these attributes. System owners should use dynamic access and approved attribute services, but may provision entitlements using explicit access where dynamic access is not supported or where attribute values are not available from approved attribute services for all users.

(d) If access to the IT resource requires specific approvals or is based on locally defined attributes, the system must implement processes to provision entitlements using explicit access.

(3) Privileged Access.

System owners must define and document roles, profiles, transactions, and other activities that are restricted to functional privileged users and IT privileged users.

(a) Functional Privileged Users.

A functional privileged user, also known as an application privileged user, is assigned a specific position or duty within an application, such as approver in a financial management system or a civilian time system. System owners may choose to use dynamic or explicit access for these users. When auditing of the provisioning process is required, system owners must provision entitlements using explicit access with an automated account provisioning system. Access by functional privileged users must be traceable to a single person or NPE.

(b) IT Privileged Users.

IT privileged users (i.e., system administrators) have access to manage IT systems and can read, write, change, download, or upload files. IT privileged users must authenticate using credentials reserved for performing privileged actions and must be provisioned using explicit access. Access by IT privileged users must be traceable to a single person or NPE.

(c) Emergency Accounts.

An emergency account grants an already privileged user temporary, exception-based, elevated access under emergency or extraordinary circumstances.

1. Organizations must establish and document policies and procedures for the use of emergency access.

2. Emergency accounts must be:

a. Provisioned using explicit access.

b. Protected at the same or higher level upon which the access was granted.

3. Use of an emergency account must:

a. Be authorized through explicit access using an auditable process.

b. Be approved in advance by a specifically designated supervisor whenever possible, or within 8 hours of its use when circumstances do not allow pre-approval.

c. Be traceable to a single person.

(4) Records Management Access.

Records management users must be authorized to access IT resources to perform records management functions including records schedule updates, rescheduling, holds, transfer, destruction, and reporting.

4.2. ACCESS REQUIREMENTS.

a. Explicit Access.

Explicit access requires provisioning authorizations, also known as entitlements, to entities for specific access rights to IT resources. Explicit access establishes a "by name" account with authorizations for each entity accessing the resource. System owners must define and document the types of access that require explicit access and the requirements for this access.

(1) Provisioning.

IT resource owners must define and document approvals necessary for users to be provisioned entitlements, including who must approve them (e.g., supervisor or security officer). System owners must implement approvals as required.

(2) Traceability.

IT resource owner must define and document process to request, approve, and provision entitlements. System owners must also document and implement a process to meet the requirement that maintains an auditable record that approvals were given before granting access.

(a) The auditable record must include the name and identifier of the user, the date of the approval, and the names and positions of approving individuals.

(b) Approval information must be retained in accordance with the requirements established in the authorization to operate documentation. Provisioning processes may be manual where necessary; however, system owners should adopt ICAM provisioning tools, such as the DoD Enterprise Automated Account Provisioning Service or DoD Component provisioning services by end of Fiscal Year 2028.

(3) De-Provisioning.

(a) IT Systems Integrated to Enterprise ICAM Person Attribute Services.

System owners and IT resource owners must provide a mechanism for users or individuals who support the approval process to request de-provisioning of entitlements when no longer required by the user to perform their job functions. Persons responsible for supervising individuals must notify the system of the need to de-provision access within 1 business day for privileged access and within 2 business days for non-privileged access.

1. For routine events (e.g., role removal, voluntary departure, termination of contract):

a. Network access permissions must be de-provisioned within 24 hours of when known to DoD Enterprise ICAM ecosystem and access is no longer authorized.

b. Physical access must be de-provisioned by the physical or building security staff by the end of the business day.

c. If notification to the system owner occurs more than 5 business days after when known to DoD Enterprise ICAM ecosystem, both network access and physical access must be de-provisioned within 1 business day of notification that access is no longer authorized.

2. For high-risk and emergency events (e.g., involuntary departure, unauthorized system use):

a. The user's Common Access Card (CAC) must be confiscated and revoked in accordance with Volume 1 of DoDM 1000.13.

b. Access must be de-provisioned as soon as possible, but no later than 2 business days after when known to DoD Enterprise ICAM ecosystem and access is no longer authorized.

c. If notification of revocation to the system owner occurs more than 2 days after the effective revocation date, access must still be de-provisioned as soon as possible.

(b) All Other IT Systems.

System owners and IT resource owners must provide a mechanism for users or individuals who support the approval process to request de-provisioning of entitlements when no longer required by the user to perform their job functions. Persons responsible for supervising individuals must notify the system of the need to de-provision access within 1 business day for privileged access and 2 business days for non-privileged access.

1. For routine events (e.g., role change, voluntary departure, termination of contract):

a. Network access permissions must be de-provisioned within 24 hours of the effective date when access is no longer authorized.

b. Physical access must be de-provisioned by the physical or building security staff by the end of the business day.

c. If notification to the system owner occurs more than 5 business days after the effective date, both network access and physical access must be de-provisioned within 1 business day of notification that access is no longer authorized.

2. For high-risk events (e.g., involuntary departure, unauthorized system use):

a. The user's CAC must be confiscated and revoked in accordance with Volume 1 of DoDM 1000.13.

b. Access must be de-provisioned as soon as possible, but no later than 2 business days after the effective date when access is no longer authorized.

c. If notification of revocation to the system owner occurs more than 2 days after the effective revocation date, access must be de-provisioned as soon as possible or within 1 business day of notification.

(4) SOD.

System owners and IT resource owners must define and document SOD requirements for users, including the definition of incompatible activities and transactions. For example, it would be a SOD violation for a functional privileged user to have both the ability to create an invoice and to authorize payment of that invoice.

(a) System owners and IT resource owners must implement automated mechanisms to verify that requests to provision entitlements for a single user that would violate SOD rules require additional approvals by the system approving official or business functional owner and auditable documentation of why the entitlements were requested and approved.

(b) System owners and IT resource owners must support enforcement of SOD requirements across systems and DoD Components by:

1. Mapping local system entitlements to enterprise roles.

2. Providing local system entitlement information to centralized auditing systems.

(5) Access Reviews.

System owners and IT resource owners must perform and document access reviews at least every 12 months for functional privileged users and at least every 3 months for IT privileged users.

(a) Access reviews must:

1. Include people authorized to use emergency accounts.

2. Verify that approvals are in place for all entitlements provisioned to active accounts.

3. Include review of SOD conflicts to verify that any users with SOD conflicts have obtained appropriate approvals.

4. Include a statement from a supervisor or system manager asserting that each user:

a. Has a specific need-to-know for classified information or a DoD purpose for controlled unclassified information.

b. Requires the entitlements to perform their job function.

(b) Access identified during the periodic reviews that exceeds what is authorized or is not supportable by a completed access request workflow must be suspended or terminated within 2 business days of notice to the system owner. All account activity must be audited for malicious activity pending adjudication and approval of the access through established access request processes.

(c) Access reviews will be performed through a provisioning tool when possible.

(d) Documentation related to access reviews must be retained for at least 12 months beyond account deactivation and be provided to auditors upon request.

b. Dynamic Access.

For dynamic access, authorization is determined when the entity requests access to the IT resource based on the digital policy rule for the resource and user and environment attribute values. Dynamic access does not require provisioning entitlements or accounts for the user.

(1) Digital Policy Rules.

IT resource owners must define digital policy rules that specify authorization requirements for dynamic access to the resource.

(a) Where digital policy rules are defined at the IT resource level, resource owners must ensure that the resource is tagged with a reference to the appropriate digital policy rule.

(b) Digital policy rules must:

1. Specify user and environmental attributes and values that must be true to grant access to the resource.

2. Include any applicable SOD requirements.

3. Include any applicable provisions regarding functional privileged users or IT privileged users.

(2) User Attributes.

System owners must obtain user attributes from approved authoritative attribute services as defined in Paragraph 4.3. and ensure that attribute values have been verified, protected from unauthorized alteration, and meet acceptable freshness for the system as described in Paragraph 4.3.a.

(3) Environmental Attributes.

System owners must obtain environmental attributes from sources that protect those attributes to prevent unauthorized alteration.

c. Hybrid Access.

(1) Use of Hybrid Access.

Systems may use a combination of explicit and dynamic access processes, either through the automated verification of user attributes as part of the provisioning process or by incorporating provisioned entitlements and additional user or environmental attributes to perform authorization.

(2) Automated Provisioning and De-Provisioning.

If automated verification of user attributes is used as part of the entitlement provisioning process for explicit access, then the provisioning process must:

(a) Subscribe to Enterprise ICAM person identity and credentialing attribute distribution services (which provide notification of changes).

(b) Re-verify critical access information, such as background investigation, clearance, and need-to-know daily.

(c) Act to de-provision the entitlement within 48 hours when changes in person attributes dictate the need.

4.3. AUTHORITATIVE ATTRIBUTE SERVICE REQUIREMENTS.

a. General.

(1) An authoritative attribute service provides user or environmental attributes to systems using dynamic access or to support automation of provisioning steps in a hybrid model.

(a) Authoritative attribute services must be approved for use at the DoD enterprise or DoD Component level and may be operated by DoD enterprise ICAM service providers, DoD Components, or external mission partners.

(b) Owners of authoritative attribute services that obtain attributes from other systems must verify that the feeder systems enforce the requirements in this issuance as part of the agreement to provide attribute values.

(2) The authoritative source for person entity attributes is DMDC's "Department of Defense Enterprise Identity Attribute Service (EIAS) Person Entity Attribute Data Set Standard."

b. Accuracy.

Owners of authoritative attribute services must define and document the processes used to verify attribute values, including the frequency with which the attribute values are refreshed. Owners of authoritative attribute services must make freshness information (i.e., assertion of the last date the data was verified) available to organizations or system owners relying on the attributes provided by the authoritative attribute service for dynamic access or automated entitlement provisioning and de-provisioning.

c. Integrity.

Attribute services must implement controls to protect attribute values commensurate with the risk level of IT resources that can be accessed based on the attributes (e.g., if attributes will be used to authorize access to moderate risk IT resources, then the attribute service must be considered moderate for integrity). Attributes must also be protected when in transit between attribute services or between attribute services and relying parties to ensure data integrity and confidentiality of attribute information.

d. Privacy and Confidentiality.

Attribute services must register relying parties and authenticate requests for attribute values to verify that the requests come from approved relying parties. Attribute services must complete privacy impact assessments and obtain appropriate System of Records Notices required by Section 552a, Title 5, United States Code (also known as "the Privacy Act of 1974"), DoDI 1000.30, and Volume 2 of DoDM 5400.11 to document the collection, storage, and use of personally identifiable information before the request for attribute services can be approved.

e. Availability.

(1) Attribute services must document the percent uptime standard either as part of their published system documentation or through service level agreements with the parties relying on the service.

(2) Authoritative attribute services must provide a mechanism to provide attributes upon a request. These attribute services should be modified to expose application programming interfaces that permit "just-in-time" queries for an entity's attributes.

4.4. AUTHORIZATION REQUIREMENTS.

a. Access Control.

System and IT resource owners must implement an authorization mechanism in addition to enforcing authentication as defined in DoDI 8520.03. The authorization mechanism may be internal or external to the system. The authorization mechanism must enforce explicit, dynamic, or hybrid access methodologies to implement defined requirements for access to resources hosted by the system. The authorization mechanism must support federated external mission partners that may be authorized and not be restricted to DoD internal community members.

b. Activity Logging.

(1) In accordance with Office of Management and Budget Memorandum M-21-31, system owners in conjunction with IT resource owners must:

(a) Define logging function requirements in accordance with Event Logging Tier 3.

(b) Develop policy and procedures to communicate events properly based on IT resource risk and mission response process.

(2) System owners must ensure the audit logs include:

(a) Logged and monitored system access by IT privileged users, including emergency access.

(b) All successful and unsuccessful requests to access identified IT resources. Logs must include the identity of the user making the request, the IT resource being requested, the date and time, and whether access was granted. For dynamic access, logs must also include the attributes used by the digital policy to determine access.

(3) System owners must implement process to review audit logs for inappropriate and suspicious activity at least weekly and report security incidents and violations to the OSD and DoD Component or USCG senior agency official for information security in accordance with DoDD 5210.50, DoDI 5200.48, and DoDM 5200.01.

(4) System owners must make access logs available to support monitoring for potential insider threats or other intrusions or instances of unauthorized access.

(5) System and IT resource privileged users must not have access to modify, add, or delete audit logs that track their activity.

c. Operationally Constrained Environments.

Systems that are operationally constrained and cannot implement network-based access control mechanisms must implement compensating controls, such as physical access controls, personnel controls, or localized access control to restrict access to authorized users.

4.5. NPE ACCESS.

a. NPEs with Static Connectivity.

NPEs may interact with each other based on static connection agreements. These agreements must include authorization information for IT resource access. Systems must implement mechanisms to enforce authorized access in accordance with static connection agreements. In addition, NPE access must be logged and monitored for unusual behavior.

b. Endpoint Device Authorization.

Access to some DoD IT resources may require authorization of the endpoint device in addition to user authorizations. Authorization of endpoint devices may be through provisioned explicit access, such as static connections described in Paragraph 4.5.a., but generally uses dynamic access. Where dynamic access is used, system owners must define and enforce digital policy rules for authorization of the endpoint based on verifiable endpoint device attributes such as the type, management state, network location, and geolocation.

c. NPEs Acting as Users.

NPEs may be processes acting as general users, IT privileged users, or functional privileged users such as service accounts, monitoring tools, and unattended robotic process automation bots.

(1) NPEs acting as users must be authorized using the same access methodologies as person users, as described in Paragraphs 4.2. and 4.4.

(2) NPEs must be provisioned with their own identities, credentials through the DoD public key infrastructure NPE issuance portal, and unique network or application accounts. NPEs must not be assigned an identifier that also maps to a person entity.

(3) To minimize duplication or mistaken access for NPE to real user accounts, unique identifiers called DoD ID numbers (per DoDI 1000.30) and last 16 digits of the Federal Agency Smart Credential Number (per Federal Information Protection Standard 201), NPEs acting as users must not contain system accounts and/or credentials with unique 10-digit or 16-digit identifiers starting with 1 through 9 for mapping to a direct access or hybrid account.

(4) Where NPE attributes are not available, NPEs must be provisioned entitlements using explicit access even if person entities use dynamic access.

(5) NPEs must not be used in a manner to circumvent SOD policy or controls. Access to NPEs should be restricted to functional privileged and user accounts that do not have conflicting SOD roles.

SECTION 5: ENTERPRISE AUTHORITATIVE ATTRIBUTE SERVICES APPROVAL PROCESSES

Enterprise authoritative attributes services must be approved for use by DoD systems in accordance with the process described in Section 4. DoD Component, USCG, or community of interest authoritative attribute services must be approved for use by the system host using the attribute service. Requests for approval must have a DoD sponsor, which may be the owner of the attribute service or a DoD Component. Approvals may be reevaluated based on changes to attribute service provider capabilities or changes in DoD risk profiles. A full list of approved enterprise authoritative attribute services is available at https://intelshare.intelink.gov/sites/dodcioicamdocs. The approvals process is as follows:

a. The sponsor must compile the following information:

(1) A description of the attribute service, including who operates it and what user community the attribute service contains information about.

(2) A list of the attributes available from the attribute service, including the name, format, and a list of possible values or description of possible values for each attribute.

(3) How the attribute service will meet the accuracy, integrity, privacy and confidentiality, and availability requirements identified in Paragraph 4.3.

(4) Interfaces supported by the attribute service to provide attributes to systems.

(5) Any restrictions on the ability of systems to obtain or use attributes from the attribute service.

(6) If the attribute service is operated by a DoD Component:

(a) Information regarding the authority to operate status of the attribute service, including any identified risks and planned remediation actions.

(b) The name of the DoD Component assigned to provide cybersecurity services for the attribute service.

(c) Information on operational testing results that includes:

1. Performance, security, stability, maintainability, accessibility, interoperability, backup, and recovery.

2. A risk assessment in accordance with the requirements from DoDI 8510.01, and planned remediation actions.

b. The sponsor submits the required information to the DoD CIO ICAM lead.

c. The DoD CIO ICAM lead coordinates a review of the request with the appropriate ICAM governance body as defined by the DoD CIO. If disapproved, the DoD CIO ICAM lead provides the sponsor with the reason the request was disapproved.

d. If recommended for approval, the DoD CIO ICAM lead develops a draft approval memorandum that includes any restrictions on the use of the attribute service.

e. The DoD CIO reviews the draft approval memorandum and signs or disapproves it.

f. If the request is approved, the DoD CIO ICAM lead provides the approval memorandum to the sponsor and adds the approval to the appropriate published list of attribute services. The DoD CIO ICAM also posts information obtained from the attribute service provider on https://cyber.mil, listing the user community and attributes supported by the attribute service and contact information for the attribute service provider.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AI	artificial intelligence
CAC	Common Access Card
CDAO	Chief Data and Artificial Intelligence Officer
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoDD	DoD directive
DoDI	DoD instruction
DoDIN	Department of Defense Information Network
DoDM	DoD manual
ICAM	identity, credential, and access management
IT	information technology
JWICS	Joint Worldwide Intelligence Communication System
NIPRNET	Non-classified Internet Protocol Router Network
NPE	non-person entity
SAP	Special Access Program
SIPRNET	SECRET Internet Protocol Router Network
SOD	separation of duties
USCG	United States Coast Guard
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

G.2. DEFINITIONS.

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

TERM — DEFINITION

access review A process used to periodically verify that only legitimate users have access to systems and IT resources.

TERM **DEFINITION**

attribute service A data repository where authorization attributes are collected and managed for a set of entities recognized as having the authority to verify the association of attributes to an identity, accessible only through a service that both provisions and serves up authorization attributes.

authentication The process by which a claimed identity is confirmed using a credential.

authorization The process by which a request to perform an action on an IT resource is decided, typically based on a policy.

digital policy rule A rule that defines the combination of attributes under which access may take place.

dynamic access The process of determining authorization when the entity requests access to the IT resource based on the digital policy rule for the IT resource and user and environment attribute values.

entitlement Authorization to access one or more IT resources within an information system.

entity A person, role, organization, device, or process that requests access to and uses IT resources.

environmental attribute A data element that describes the situation at the time of the transaction, such as time of day, external event occurrence, physical location of the entity making the request, or threat level.

explicit access The process of provisioning authorizations, known as entitlements, to entities for specific access rights to IT resources.

functional privileged user A user who has approval authorities within workflows. Functional privileged user roles are specific to a mission area, such as human resources or finance.

general user A user who does not have elevated privileges of a functional privileged user or IT privileged user.

TERM	DEFINITION
IT privileged user	A user that 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.
IT resource	Includes all the equipment, networks, hardware, software, technical knowledge, expertise, and other resources – including all IT resources and computer systems – held, owned, or used by or on behalf of the DoD.
mission partner	An organization with which the DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government; State and local governments; allies, coalition members, host nations and other nations; multinational organizations; non-governmental organizations; and the private sector.
national security system	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency.
NPE	A physical device, virtual machine, system, service, or process that is assigned an identifier and issued credentials to support authentication and authorization.
privileged user	A user that is authorized (and therefore, trusted) to perform security relevant functions that ordinary users are not authorized to perform. (Also see IT privileged user, functional privileged user)
provisioning	Linking and unlinking access permissions for a person or NPE to a protected IT resource.
service account	An NPE account created to execute applications and run automated services and other processes.
system	Defined in the Committee on National Security Systems Instruction 4009.

REFERENCES

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems (CNSS) Glossary," March 2, 2022

Defense Manpower Data Center, "Department of Defense Enterprise Identity Attribute Service (EIAS) Person Entity Attribute Data Set Standard," current edition[1]

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

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

DoD Directive 5205.02E, "DoD Operations Security," June 20, 2012, as amended

DoD Directive 5210.50, "Management of Serious Security Incidents Involving Classified Information," September 18, 2020, as amended

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

DoD Instruction 5200.02, "DoD Personnel Security Program," March 21, 2014, as amended

DoD Instruction 5200.46, "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)," September 9, 2014, as amended

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

DoD Instruction 5210.83, "DoD Unclassified Controlled Nuclear Information (UCNI)," July 12, 2012, as amended

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019, as amended

DoD Instruction 5230.24, "Distribution Statements on DoD Technical Information", January 10, 2023

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

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

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 18, 2023

DoD Instruction 8520.03, "Identity Authentication for Information Systems," May 19, 2023

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

DoD Instruction 8910.01, "DoD Implementation of the Paperwork Reduction Act," December 5, 2022

[1] Available at https://go.intelink.gov/2xiZ0SP.

DoD Manual 1000.13, Volume 1, "DoD Identification (ID) Cards: ID Card Life-Cycle," January 23, 2014, as amended

DoD Manual 5200.01, Volumes 1-3, "DoD Information Security Program," dates vary by volume

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 by Executive Order 13526, December 29, 2009, and Executive Order 14086, October 7, 2022

Federal Information Protection Standard 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors," current edition[2]

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 17, 2017

Office of the DoD Chief Information Officer, "Department of Defense Identity, Credential, Management and Access (ICAM) Strategy Classification: Unclassified," March 30, 2020[3]

Office of the DoD Chief Information Officer, "DoD Enterprise Identity, Credential, and Access Management (ICAM) Reference Design," June 2020[3]

Office of the DoD Chief Information Officer, "Adoption of Initial DoD Identity, Credential, and Access Management Enterprise Services," May 2023[3]

Office of the DoD Chief Information Officer, "DoD Zero Trust Reference Architecture," July 2022[3]

Office of the DoD Chief Information Officer, "DoD Zero Trust Strategy," October 21, 2022[3]

Office of Management and Budget Memorandum M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," August 27, 2021

United States Code, Title 5, Section 552a (also known as the "Privacy Act of 1974")

United States Code, Title 42, Chapter 23, Division A (also known as the "Atomic Energy Act," as amended)

[2] Available at https://csrc.nist.gov/publications/fips.

[3] Available at https://cyber.mil/icam/document-library/.