Department of Defense

INSTRUCTION

NUMBER 8520.03
May 13, 2011

ASD(NII)/DoD CIO

SUBJECT: Identity Authentication for Information Systems

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.1 (Reference (a)), this Instruction:

a. Implements policy in DoDD 8500.01E (Reference (b)), assigns responsibilities, and prescribes procedures for implementing identity authentication of all entities to DoD information systems.

b. Establishes policy directing how all identity authentication processes used in DoD information systems will conform to Reference (b) and DoD Instruction (DoDI) 8500.2 (Reference (c)).

c. Implements use of the DoD Common Access Card, which is the DoD personal identity verification credential, into identity authentication processes in DoD information systems where appropriate in accordance with Deputy Secretary of Defense Memorandum (Reference (d)).

d. Aligns identity authentication with DoD identity management capabilities identified in the DoD Identity Management Strategic Plan (Reference (e)).

e. Establishes and defines sensitivity levels for the purpose of determining appropriate authentication methods and mechanisms. Establishes and defines sensitivity levels for sensitive information as defined in Reference (b) and sensitivity levels for classified information as defined in DoD 5200.1-R (Reference (f)).

2. APPLICABILITY

a. This Instruction 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 the Inspector General of the

DoD, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereinafter referred to collectively as the "DoD Components").

(2) All DoD unclassified and classified information systems including networks (e.g., non-classified Internet Protocol Router Network, Secret Internet Protocol Router Network (SIPRNET)), Defense Research and Engineering Network, Secret Defense Research and Engineering Network web servers, and e-mail systems.

(3) All DoD and non-DoD personnel entering or exiting DoD facilities or installations that authenticate to a physical access control system (PACS).

(4) All DoD and non-DoD entities (human and non-person) logically accessing DoD unclassified and classified information systems including, but not limited to, DoD web-based systems, DoD websites, DoD web servers, and DoD networks. Hereinafter in this Instruction, use of "entities" refers to human and non-person users.

b. This Instruction does NOT apply to:

(1) Unclassified internet-based systems specifically intended to engage DoD mission partners, known and unknown, in nontraditional missions such as humanitarian assistance, disaster response, stability operations, or building partner capacity.

(2) Sensitive Compartmented Information and information systems operated within the DoD that fall under the authority provided in Intelligence Community Directive 503 (Reference (g)). This Instruction also does not apply to Top Secret collateral systems, special access programs, and stand-alone networks with no connection to the Global Information Grid.

3. DEFINITIONS. See Glossary.

4. POLICY. It is DoD policy in accordance with Reference (b) that:

a. All DoD information systems or DoD networks that either host information that has not been approved for public release in accordance with DoDD 5230.09 and DoDI 5230.29 (References (h) and (i)) or electronically facilitate physical access to DoD facilities shall authenticate all entities as specified in this Instruction prior to granting access.

(1) The information system or DoD network shall ensure that any credential used for identity authentication is appropriate for the authenticating entity's environment or physical location and the sensitivity level of the information or force protection level of the facility or other resources for which the information system facilitates access or privilege. This Instruction provides criteria and methodology for determining appropriate identity credentials for authentication in Enclosure 3.

(2) The information system or DoD network shall ensure that any credential used for identity authentication has been issued by an approved DoD identity credential provider or a DoD-approved Federal or industry partner identity credential provider.

(3) The information system or DoD network shall verify that any identity credential used for identity authentication has not been revoked by the identity credential provider or otherwise declared invalid. In situations where the automated mechanisms used for revocation checking are not available (e.g., on-line certificate status protocol responses from the Robust Certificate Validation Service or certificate revocation lists (CRLs) from the Global Directory Service), systems or networks will perform credential revocation checking in accordance with the applicable credential policy (e.g., cached CRLs) or a documented standard operating procedure.

b. The information system or DoD network shall validate during logon that the authenticator (the value or data object used to prove the claimant possesses and controls the identity credential) is bound to the identity credential used in the identity authentication process.

c. DoD information systems or DoD networks granting access to entities using non-DoD controlled computers (i.e., not Government-furnished) or non-DoD networks shall ensure the identity credential used and sensitivity level of the information or other resources for which the information system facilitates access are appropriate for the non-DoD system or non-DoD network environment from which the identity authentication session initiates. This Instruction provides criteria for determining appropriate authentication methods and mechanisms.

d. All DoD information systems or DoD networks that host any information that has not been approved for public release in accordance with References (h) and (i) shall implement rules-based processes for:

(1) Mapping an authenticated identity to a network or information system account or role.

(2) Granting or denying access to information based on the authorizations associated with an account or role.

(3) Disabling, suspending, or removing accounts when access is no longer authorized.

(4) Terminating access to the related application account(s) when a role changes or is terminated. This may be accomplished through rules or through documented standard operating procedures.

e. As the capability to execute dynamic rules-based or attribute-based access control becomes available, DoD Component-appointed designated accrediting authorities (DAAs) may authorize its use as appropriate.

f. Operators of DoD networks and information systems shall develop and document the procedures for managing access control, including procedures for making authorization decisions when the primary access control mechanisms are unavailable.

g. DoD information systems or DoD networks shall authenticate devices (non-person users) that connect to them during the course of their operations or processing, as specified in this Instruction, prior to granting connection or access.

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. EFFECTIVE DATE. This Instruction is effective upon its publication to the DoD Issuances Website.

Teri M. Takai
Acting Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

Enclosures:
1. References
2. Responsibilities
3. Implementation Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005
(b) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
(d) Deputy Secretary of Defense Memorandum, "DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12)," November 26, 2008
(e) Deputy Secretary of Defense Strategy, "DoD Identity Management Strategic Plan," April 2009[1]
(f) DoD 5200.1-R, "Information Security Program," January 14, 1997
(g) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
(h) DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008
(i) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," January 8, 2009
(j) DoD Directive 1000.25, "DoD Personnel Identity Protection (PIP) Program," July 19, 2004
(k) Under Secretary of Defense for Intelligence Directive-Type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009
(l) DoD Directive 8521.01E, "Department of Defense Biometrics," February 21, 2008
(m) Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Plan, "Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy," August 2009[2]
(n) Section 3541 et. seq. of title 44, United States Code
(o) DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
(p) DoD Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011
(q) Section 552a of title 5, United States Code
(r) Section 264 of Public Law 104-191, "The Health Insurance Portability and Accountability Act of 1996," August 21, 1996
(s) Section 552 of title 5, United States Code
(t) Federal Information Processing Standards Publication 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004
(u) National Institute of Standards and Technology Special Publication 800-60, Volume 1, revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008
(v) National Institute of Standards and Technology Special Publication 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", April 2010

[1] https://www.us.army.mil/suite/files/14352077

[2] https://www.us.army.mil/suite/doc/19813448

(w) National Institute of Standards and Technology Special Publication 800-63 version 1.0.2, "Electronic Authentication Guideline," April 2006
(x) Federal Information Processing Standards Publication 201-1, "Personal Identity Verification for Federal Employees and Contractors," March 2006
(y) Federal Public Key Infrastructure Policy Authority, "X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA)," current edition
(z) Committee on National Security Systems Policy No. 25, "National Policy for Public Key Infrastructure in National Security Systems," March 2009
(aa) DoD 5200.2-R, "Personnel Security Program," January 1987
(ab) Chairman of the Joint Chiefs of Staff Instruction 6211.02C, "Defense Information System Network (DISN): Policy and Responsibilities," July 9, 2008
(ac) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, "DoD External Interoperability Plan," June 2009[3]

[3] https://www.us.army.mil/suite/page/571419

ENCLOSURE 2

RESPONSIBILITIES

1. ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DoD CHIEF INFORMATION OFFICER (ASD(NII)/DoD CIO). The ASD(NII)/DoD CIO, in addition to the responsibilities in section 6 of this enclosure, shall:

a. Develop identity authentication policy and guidance for DoD information systems and networks.

b. Provide guidance to facilitate the management and implementation of identity authentication processes and procedures used when gaining access to information systems and networks.

c. Approve DoD relying party use of identity credentials with Credential Strengths A, B, C, D, E, F, G, and H (see section 3 of Enclosure 3) upon the advice and coordination of the Identity Protection and Management Senior Coordinating Group, including:

(1) Establishing and administering an accreditation program for identity credential providers and their services.

(2) Maintaining and making available to all DoD information systems an authoritative list of identity credential providers and identity credential services approved for use with DoD information systems.

d. Oversee identity authentication compliance efforts (see section 9 of Enclosure 3).

e. When appropriate, coordinate with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and the Under Secretary of Defense for Intelligence (USD(I)) on the approval process for identity credentials and identity credential providers.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). The Director, DISA, under the authority, direction, and control of the ASD(NII)/DoD CIO and in addition to the responsibilities in section 6 of this enclosure, shall:

a. Provide technical support to the Heads of the DoD Components when they are implementing procedures in this Instruction.

b. Maintain an authoritative list of all identity credential solutions approved for use in identity authentication processes and the technical characteristics pertaining to each. Provide subject matter expertise and technical consultation to information systems on matters relating to authentication processes.

3. USD(P&R). The USD(P&R), pursuant to Reference (b) and DoDD 1000.25 (Reference (j)), and in addition to the responsibilities in section 6 of this enclosure, shall, when appropriate, coordinate with the ASD(NII)/DoD CIO and the USD(I) on the approval process for identity credentials and identity credential providers.

4. USD(I). The USD(I), pursuant to Directive-Type Memorandum 09-012 (Reference (k)), and in addition to the responsibilities in section 6 of this enclosure, shall:

a. Designate identity credentials approved for use for identity authentication to PACS.

b. Coordinate with the ASD(NII)/DoD CIO and the USD(P&R) on identity credential approval.

5. ASSISTANT SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING (ASD(R&E)). In addition to the responsibilities in section 6 of this enclosure, the ASD(R&E), under the authority, direction, and control of the Under Secretary of Defense for Acquisition, Technology, and Logistics in accordance with DoDD 8521.01E (Reference (l)), shall:

a. Oversee the DoD Biometrics Executive Manager-led biometric identity credential standards and accreditation program.

b. Coordinate with the ASD(NII)/DoD CIO, the USD(P&R), and the USD(I) on approval of identity credentials that include biometric factors.

6. HEADS OF THE OSD AND DoD COMPONENTS. The Heads of the OSD and DoD Components shall:

a. Plan, program, and budget to support the identity authentication processes for Component information systems and networks.

b. Ensure proper use of identity authentication processes for all Component information systems and networks.

c. Ensure Component identity authentication processes are synchronized with the Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy (Reference (m)) and are aligned with DoD information assurance (IA) policies (including certification and accreditation, computer network defense, and reporting required by section 3541 et. seq. of title 44, United States Code (also known as the Federal Information Security Management Act (Reference (n)) and privilege management initiatives.

d. Designate an office responsible for coordinating identity authentication activities across their respective Component.

e. Develop and implement policies and procedures for use of DoD-approved public key infrastructure (PKI) certificates in PKI-based identity authentication processes for Component business and mission processes.

f. Appoint Component-approved DAAs to approve acceptance of risk in certification and accreditation activities in alignment with DoDI 8510.01, (Reference (o))

7. CHAIRMAN OF THE JOINT CHIEFS OF STAFF. The Chairman of the Joint Chiefs of Staff, in accordance with Reference (b) and in addition to the responsibilities in section 6 of this enclosure, shall:

a. Identify, review, and validate the identity authentication processes used by systems or applications that provide support for joint, allied, and/or coalition missions.

b. Require the Combatant Commanders coordinate processes to implement this Instruction with their host Military Departments in accordance with DoDD 5100.03 (Reference (p)).

ENCLOSURE 3

IMPLEMENTATION PROCEDURES

1. INTRODUCTION

a. Identity authentication for information systems and networks within the DoD must be conducted in a manner that provides confidentiality by mitigating against unauthorized access; provides integrity that protects against unintentional or malicious change; and provides availability of data for all DoD mission partners and users. To perform proper authentication, information system owners must use identity authentication procedures that consider the importance and sensitivity of the information in a system, recognize the threats and vulnerabilities to the system, consider the level of confidence in any user's asserted identity, and the impairment or destruction that could be inflicted on the information system, as stated in paragraph 4.2 of Reference (b). For physical facilities, identity authentication procedures should consider the force protection condition of the facility, recognize the threats and vulnerabilities against the location, the level of confidence of the entrant's asserted identity, and the disruption or destruction that could be inflicted at the DoD facility or location.

b. To conduct reliable identity authentication, information system owners and persons responsible for allowing access to physical facilities or locations shall choose the specific type(s) of identity credential used in an identity authentication process based on the sensitivity of the information or facility that can be accessed, the strength of the identity credential, and the environment or location where the identity credential is being presented. These three criteria are discussed in more depth in this enclosure.

2. SENSITIVITY LEVELS

a. General. Sensitivity levels relate the relative importance of information residing in a system or on a network to the potential impact that could be caused by unauthorized access or modification of that information. The types of information residing in an information system or on a network that may be considered sensitive include, but are not limited to:

(1) Personally sensitive information such as medical records, credit card numbers, job applications, and training reports, which are considered sensitive because of their personal nature.

(2) Business sensitive information that is provided by a source or sources, such as a commercial or foreign government partner, under the condition that it not be released to other parties.

(3) Regulatory sensitive information that has been designated by law, regulation, or other mandate as sensitive information. This information includes personally identifiable information protected under section 552a of title 5 United States Code (also known as the Privacy Act of

1974 (Reference (q)), individually identifiable health information protected according to section 264 of Public Law 104-191 (also known as the Health Insurance Portability and Accountability Act of 1996) (Reference (r)), information exempted from mandatory public disclosure according to section 552 of title 5, United States Code (also known as the Freedom of Information Act) (Reference (s)), and data that is subject to export controls.

(4) Operations sensitive information, the loss, misuse, or unauthorized access to or modification of which could adversely affect DoD missions, the national interest, or the conduct of Federal programs. This includes information in routine DoD payroll, finance, logistics, and personnel management systems.

(5) Combat mission sensitive information that is critical to a DoD combat or strategic mission, such that unauthorized access to or compromise of this information could result in severe mission capability degradation, major damage to DoD assets, or a risk of serious injury or death to personnel involved with the mission.

b. Categorizing Information and Information Systems. Information system owners should refer to Federal Information Processing Standards (FIPS) Publication 199 (Reference (t)), National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 (Reference (u)) and NIST SP 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" (Reference (v)) for a framework for conducting information categorization. Sensitivity levels may be identified for unclassified and classified information.

c. Sensitivity Levels for Unclassified Information. There are four sensitivity levels that apply to the categories of information defined as "sensitive" in paragraph E2.1.41 of Reference (b). Sensitive information shall be automatically categorized as Sensitivity Level 3 unless the information owner determines that the data meets the criteria for Levels 1, 2, or 4. Information that has been approved for public release in accordance with References (h) and (i) will not be considered to have a sensitivity level.

(1) Sensitivity Level 1. Information that is considered sensitive because it is personal in nature, pertains to only a single individual, and would have a low adverse impact on the efficacy of DoD missions if the information were compromised (e.g., lost; misused; or accessed, modified, or distributed without authorization). Examples of this information include an individual's own medical record, credit card numbers, job application, and training record. The personal information of multiple individuals, in aggregate, should be considered Sensitivity Level 3.

(2) Sensitivity Level 2. Information that is considered sensitive because it has been provided by a source or sources (e.g., Federal, State, or local government; a foreign government; or a commercial organization) under the condition that it not be released to other parties and would have a low or moderate adverse impact on the efficacy of DoD missions or the reputation of the DoD if the information were compromised. Examples of this information include contract documents between commercial companies and the DoD or a company's proprietary information or trade secrets.

(3) Sensitivity Level 3. Information that could adversely affect DoD mission interests and would have a moderate or high impact on the efficacy of DoD missions if the information were compromised. Examples of this information include that which is available in DoD payroll, finance, logistics, and personnel management systems or information for which access is limited by law, regulation, or other mandate.

(4) Sensitivity Level 4. Information that is critical to DoD missions, such that unauthorized access to or compromise of this information could result in severe mission capability degradation, major damage to DoD information based resources, or a risk of serious injury or death to personnel, but that has not been specifically authorized to be classified in the interest of national defense or foreign policy under criteria established by Executive order or an Act of Congress.

d. Sensitivity Levels for Classified Information. There are three sensitivity levels that apply to information that is classified as Secret or Confidential in accordance with Reference (f). Classified information shall be categorized as Sensitivity Level 5 information unless the information owner deems the data to meet the criteria for either Level 6 or 7.

(1) Sensitivity Level 5. Information that is approved for access by all potential users of the classified network on which the information resides (e.g., SIPRNET), including users accessing the network from DoD mission partner classified networks through network connectivity agreements.

(2) Sensitivity Level 6. Information that carries additional precautionary data handling caveats or dissemination limitations (e.g., not releasable to foreign nationals). The handling or dissemination requirements of Sensitivity Level 6 associate greater risk than with Sensitivity Level 5 information within the classified network on which the information resides (e.g., SIPRNET).

(3) Sensitivity Level 7. For Sensitivity Level 7, the data or system owner has determined that to enhance the information security protections afforded to classified data in accordance with Reference (f), the type and strength of the identity credential used for identity authentication and the user's authentication environment must be verified by the information system during the identity authentication process before authorization to Sensitivity Level 7 information is granted.

3. CREDENTIAL STRENGTH

a. General. Credential strength is a characteristic of an identity credential that indicates the resistance of the identity credential to forgery or fraudulent use, taking into account the strength of the identity credential technology, the rigor of the identity proofing performed prior to issuance of the identity credential, and the protections incorporated into the process for issuing and managing the identity credential's life cycle. Credential strengths are established for unclassified and classified environments. Incorporation of additional authentication factors (e.g., biometrics) into system identity authentication processes is authorized where the relying party in the identity authentication process deems an enhanced strength of identity credential is necessary

or desirable. A biometric identifier (e.g., a fingerprint, an iris scan, or a hand geometry template) that is registered in a DoD-approved authoritative source and is used as an enabler (i.e., as one factor of an approved multi-factor identity authentication process) with any credential strength described in this Instruction is approved in accordance with Reference (l).

b. Credential Strengths for Use in Unclassified Environments. There are five credential strengths that are used in unclassified environments. These are enumerated in relation to the e-authentication assurance levels identified in NIST SP 800-63 (Reference (w)) and the identity credential issuance and management models identified in FIPS Publication 201-1 (Reference (x)). Additional information about e-authentication levels is in the Glossary.

(1) Credential Strength A. These identity credentials use the credential technologies and comply with the identity proofing, registration and credential management requirements defined in Reference (w) for e-authentication level 2. These credentials shall meet minimum password length and complexity requirements defined in Reference (c). They are issued by an identity credential service provider that has fully documented the system and security requirements implemented for identity credential issuance and management.

(2) Credential Strength B. These identity credentials use the credential technologies and comply with the identity proofing, registration and credential management requirements defined in Reference (w) for e-authentication level 3. Credential Strength B credentials can use either a multi-token solution or a multi-factor one-time password solution. These credential solutions do not involve the use of public key cryptography or PKI certificates. These credentials are issued by an identity credential service provider that has fully documented the system requirements for identity credential issuance and management and that is audited by an independent third party at least once every 3 years to ensure compliance with its documentation.

(3) Credential Strength C. These identity credentials use a software-based PKI technology and comply with the identity proofing, registration, and credential management requirements defined in Reference (w) for e-authentication level 3. These identity credentials are issued by an identity credential service provider that has been certified or accredited against a standard such as the Certificate Policy for the Federal Bridge Certification Authority (Reference (y)), and that is audited by an independent third party at least once every 3 years to ensure compliance with its documentation.

(4) Credential Strength D. These identity credentials use a hardware token technology and comply with the identity proofing, registration, and credential management requirements defined in Reference (w) for e-authentication level 4. Credential Strength D credentials can use either multi-factor one-time password or PKI certificate technology solution. These identity credentials are issued by an identity credential service provider that has been certified or accredited against a standard (e.g., a recognized PKI bridge certificate policy, a Federal information processing standard, or a document from an international standards body). PKI certificate technology solutions shall be cross-certified with Reference (y) at medium hardware assurance or high assurance, or an equivalent certificate policy as approved by the ASD(NII)/DoD CIO, and shall be audited by an independent third party at least once every 3

years to ensure compliance with its documentation.

(5) Credential Strength E. These identity credentials use a hardware token PKI technology and comply with the identity proofing, registration, and credential management defined in Reference (w) for e-authentication level 4. In addition, the subscriber's identity shall have been proofed and vetted in accordance with Reference (x). These identity credentials are issued by an identity credential service provider that is either a Federal agency, an approved shared service provider under the Federal PKI Policy Authority Program, or an identity credential service provider that has been specifically approved by the ASD(NII)/DoD CIO as a Credential Strength E service provider. The identity credential service provider is also audited by an independent third party at least once every 3 years to ensure compliance with its documentation.

c. Credential Strengths for Use in Classified Environments. There are three credential strengths that are used in classified environments.

(1) Credential Strength F. These identity credentials use the credential technologies and comply with the identity proofing, registration and credential management defined in Reference (w) for e-authentication level 2 and meet minimum password length and complexity requirements defined in Reference (c).

(2) Credential Strength G. These identity credentials use software PKI technology and have been issued by an identity credential service provider that is either a member of the National Security Systems (NSS) PKI, is cross-certified with the NSS PKI as described in Committee on National Security Systems (CNSS) Policy No. 25 (Reference (z)), or has been specifically approved by ASD(NII)/DoD CIO as a Credential Strength G service provider.

(3) Credential Strength H. These identity credentials have hardware PKI technology and have been issued by an identity credential service provider that is either a member of the NSS PKI, is cross-certified with the NSS PKI as described in Reference (z), or has been specifically approved by ASD(NII)/DoD CIO as a Credential Strength H service provider.

d. List of Identity Credentials and Providers. The Director, DISA, will maintain an authoritative and web-accessible list of approved identity credentials and identity credential providers at https://www.us.army.mil/suite/page/571419.

4. ENTITY ENVIRONMENT. The specific environment (i.e., the connectivity medium and the computer) from which any entity may initiate an authentication session must be considered when selecting the appropriate or required identity credential for identity authentication to a system or network by a user or group of users. The environment where an authentication session initiates includes the physical location of the user's computing platform (e.g., a home office, telecommuting center, DoD mission partner office, DoD office facility), the logical location or environment of the computing platform (e.g., commercial ISP in an internet café, DoD mission partner's internal network, a DoD office), the computing platform (e.g., a personal home computer, public library workstation, DoD mission partner laptop, government furnished laptop,

Blackberry, or Secure Mobile Environment Personal Electronic Device (SME-PED)), and the computing platform's operating system integrity and resilience against unintentional or unauthorized modification.

a. Unclassified Entity Environments. There are five unclassified entity environments. In these environments, where there is no physical connection (e.g., an RJ-45 connector into a local area network) to a DoD network, any logical connection to DoD networks will be made using technologies (e.g., virtual private network (VPN)) approved for use in applicable security technical implementation guides (STIGs).

(1) DoD Network. In the DoD network environment, a computing asset (e.g., a workstation or laptop) is owned or operated on behalf of the DoD, physically connected to a DoD unclassified network, and physically located on DoD premises.

(2) DoD Managed. In the DoD managed environment, a computing asset is owned or operated on behalf of the DoD, but not physically connected to a DoD network. Logon to a DoD unclassified network from a DoD managed environment must use technologies (e.g., VPN) approved for use in applicable STIGs.

(3) Partner Managed. In the partner managed environment, a computing asset is owned and managed by a DoD mission partner and not physically connected to a DoD network.

(4) User Managed. In the user managed environment, a personally owned computing asset is used to initiate an authentication session (i.e., the owner has control of the maintenance of the hardware and software configuration).

(5) Untrusted. In the untrusted environment, a computing asset (e.g., a public library computer) cannot be verified by a DoD computing environment or application acting as a relying party as being under the management or control of the DoD, a DoD mission partner, or an individual.

b. Classified Entity Environments. There are two classified entity environments. Both environments are assumed to operate on the DoD SIPRNET.

(1) DoD Network. In the DoD network environment, a computing asset is owned or operated on behalf of the DoD, physically connected to a DoD classified network, and physically located on DoD premises.

(2) Partner Network. In the partner network environment, a computing asset is owned or operated on behalf of the DoD, physically connected to a network owned and managed by the DoD, but physically located at the premises of a DoD mission partner.

5. AUTHENTICATING HUMAN USERS FOR ACCESS TO INFORMATION. The figure and sections 5 and 6 of this enclosure stipulate the minimum appropriate credential strength for humans authenticating to information systems including PACS. For some sensitivity levels, the

minimum appropriate credential strength differs depending on the entity environment from which the identity credential is presented. For all sensitivity levels, information systems will support identity authentication using all credential strengths that meet or exceed the minimum identified.

Figure. Minimum Credential Strengths for Authentication to Information Systems

		Entity Environment						
		Untrusted	User Managed	Partner Managed	DoD Managed	DoD Network	Classified Partner Network	Classified DoD Network
Sensitivity Level	Classified 7						**H**	**H**
	Classified 6						**G**	**G**
	Classified 5						**F**	**F**
	Admin Accounts			**E**	**E**	**E**	**H**	**H**
	Unclassified 4			**E**	**E**	**E**		
	Unclassified 3		**D**	**C**	**C**	**B**		
	Unclassified 2		**D**	**B**	**B**	**A**		
	Unclassified 1	**A**	**A**	**A**	**A**	**A**		

Key
Letters indicate minimum credential strength to be used for each combination of the entity environment and sensitivity level

a. Authenticating to Information Systems Processing Unclassified Information

(1) Information systems hosting Sensitivity Level 1 information shall be required to use an identity credential that meets or exceeds Credential Strength A when authenticating users that are accessing Sensitivity Level 1 information from an untrusted, user managed, partner managed, DoD managed, or DoD network environment.

(2) Information systems hosting Sensitivity Level 2 information shall be required to use an identity credential that:

(a) Meets or exceeds Credential Strength D when authenticating users that are accessing Sensitivity Level 2 information from a user managed environment.

(b) Meets or exceeds Credential Strength B when authenticating users that are accessing Sensitivity Level 2 information from partner managed or DoD managed environments.

(c) Meets or exceeds Credential Strength A when authenticating users that are accessing Sensitivity Level 2 information from a DoD network environment.

(3) Information systems hosting Sensitivity Level 3 information shall be required to use an identity credential that:

(a) Meets or exceeds Credential Strength D when authenticating users that are accessing Sensitivity Level 3 information from a user managed environment.

(b) Meets or exceeds Credential Strength C when authenticating users that are accessing Sensitivity Level 3 information from partner managed or DoD managed environments.

(c) Meets or exceeds Credential Strength B when authenticating users that are accessing Sensitivity Level 3 information from a DoD network environment.

(4) Information systems hosting Sensitivity Level 4 information shall be required to use an identity credential that meets Credential Strength E when authenticating users that are accessing Sensitivity Level 4 information from a partner managed, DoD managed, or DoD network environment.

(5) Information systems with administrative accounts and other accounts or roles that authorize entities access to data regardless of sensitivity level within a system shall be required to use an identity credential that meets Credential Strength E when authenticating administrative users that are accessing the system from a partner managed, DoD managed, or DoD network environment.

(a) Information systems with administrative accounts that do not accommodate the use of an identity credential that meets Credential Strength E will authenticate using IA principles and best practices (e.g., 15 character passwords for Microsoft Windows service accounts) to mitigate known or anticipated vulnerabilities. (All references to "Windows" within this Instruction refer to Microsoft Windows.)

(b) Administrative accounts shall not be accessed from an untrusted or user managed environments.

b. Authenticating to Information Systems Processing Classified Information

(1) Information systems hosting Sensitivity Level 5 information shall be required to use an identity credential that meets or exceeds Credential Strength F when authenticating users that are accessing Sensitivity Level 5 information from a partner network or DoD network environment.

(2) Information systems hosting Sensitivity Level 6 information shall be required to use an identity credential that meets or exceeds Credential Strength G when authenticating users that are accessing Sensitivity Level 6 information from a partner network or DoD network environment.

(3) Information systems hosting Sensitivity Level 7 information shall be required to use an identity credential that meets Credential Strength H when authenticating users that are

accessing Sensitivity Level 7 information from a partner network or DoD network environment.

(4) Information systems with administrative accounts or other accounts or roles that authorize entities access to data regardless of sensitivity level of the data shall be required to use a minimum of Credential Strength H when authenticating administrative users that are accessing the system from a partner network or a DoD network environment. For information systems with administrative accounts that do not accommodate the use of an identity credential that meets Credential Strength H, information systems will apply IA principles and best practices (e.g., 15 character passwords for Windows service accounts) to mitigate known or anticipated vulnerabilities.

c. Identity Authentication to PACS Peripherals for Access to Physical Facilities

(1) In physical facilities or installations where people use identity credentials for identity authentication to gain access, PACS shall require an identity credential that meets or exceeds Credential Strength A to authenticate a person's identity to PACS operating in a partner managed, DoD managed, or DoD network environment. Until electronic validation of identity credentials is available, physical and visual inspection of identity credentials must be employed in accordance with applicable DoD policy and the DoD Component's procedures.

(2) Administrative accounts or other accounts or roles for PACS identity management databases that authorize a person access to data regardless of sensitivity level of the data shall be required to use a minimum of Credential Strength E when authenticating administrative users accessing the PACS from a partner managed, DoD managed, or DoD network environment. Administrative accounts shall not be accessed from an untrusted or user managed environment.

d. Identity Authentication Under Non-standard Conditions or During Contingency Operations

(1) There exist transitional or temporary conditions during which business processes or mission execution require deviation from normal identity authentication procedures for limited periods of time. To the extent possible, information systems owners should plan for and establish standard procedures for identity authentication under temporary or exigent conditions including, but not limited to, continuity of operations and continuity of Government scenarios, identity credentials that cannot be replaced or reissued in a timely manner, lost or stolen identity credentials, or force protection or information operations conditions. Temporary procedures should incorporate best security practices and align with Reference (c).

(2) DoD Components will establish, publish, and execute procedures for identity authentication to systems under non-standard conditions. Additional risks posed by non-standard conditions must be mitigated and the DoD Component must have reviewed and approved the procedures. Documented DoD Component approved procedures do not require a waiver of this policy.

e. Use of Biometrics in Identity Authentication. Biometrics, as part of authorized identity authentication procedures, may be used in electronic information systems. Information system

owners are authorized to use a biometric identifier as an additional authentication factor (i.e., as one factor of an approved multi-factor authentication solution) with any credential strength described in this Instruction. At the discretion of the information system owner, biometrics may be used as one of the authentication factors where at least a total of two factors are used in a process to authenticate to an information system.

6. AUTHENTICATING HUMAN USERS TO DoD NETWORKS

a. Network Logon. Identity authentication for logon to a DoD network requires Credential Strength E for unclassified networks and Credential Strength H for classified networks applicable in this Instruction. Network logon shall be performed from a DoD network or DoD managed environments and shall never be performed from untrusted environments. Partner managed environments should not require DoD network logon as these users should be authenticating to their respective partner networks. The trustworthiness or suitability determination required for an individual to be granted a DoD network account should be in line with the background investigation requirement for conducting computer activities, as specified in paragraph C3.6.15 of DoD 5200.2-R (Reference (aa)).

b. Network Logon from a User Managed Environment. Network logon can only be permitted from a user managed environment if it is not practical to provide a DoD managed computing platform (i.e., a laptop that complies with all applicable DoD STIGs) to perform a DoD business activity. Network logon from a user managed environment shall be authorized by the Head of a DoD Component or a designated authority. Users authorized to perform network logon from a user managed environment shall be provided with specific instructions and tools (e.g., a Component-approved Virtual Machine capability) from the sponsoring DoD Component organization for protection and isolation from the user managed computer.

c. Network Logon Using Non-Windows Operating Systems. Network logon using non-Windows operating systems (e.g., LINUX, UNIX, Sun Solaris, Apple) shall use Credential Strength E identity credentials to the greatest extent possible. DoD Component DAAs shall approve identity credentials (other than Credential Strength E credentials) and procedures required for use by users authenticating to non-Windows systems based on a balance between risk and mission and operational requirements.

7. AUTHENTICATING SYSTEMS OR DEVICES TO NETWORKS OR OTHER SYSTEMS OR DEVICES

a. Regardless of sensitivity level, information systems hosting sensitive information (i.e., the relying party) shall require authenticating systems or devices (i.e., the subscribing party) to provide an identity credential that meets or exceeds Credential Strength A when they are authenticating from user managed, partner managed, DoD managed, or DoD network environments. When the subscribing party has the capability to assert its identity using PKI certificates, the relying party shall require authentication using an identity credential that meets

or exceeds Credential Strength B.

b. Regardless of sensitivity level, information systems hosting classified information shall require authenticating systems or devices to provide an identity credential that meets or exceeds Credential Strength F when they are authenticating from partner network or DoD network environments.

c. Devices shall execute device authentication (e.g., device-to-device or device-to-network controller) using Credential Strength C (in unclassified environments) or Credential Strength G (in classified environments) on any device when that device's capability allows for use of PKI certificates. Devices that do not support PKI-based authentication shall employ device authentication in accordance with best commercial practices until such time as the PKI-based capability is available.

8. WAIVERS

a. The Defense Information System Network/Global Information Grid (DISN/GIG) Flag Panel may authorize waiving compliance with this Instruction for individual information systems on a case-by-case basis. Waivers shall be granted only for the minimum length of time required to achieve compliance. All waiver requests from information systems or their operational control headquarters or program office will include an endorsement memorandum from the DoD Component Chief Information Officer that validates the waiver rationale and justification. An information system applying for a waiver to this policy will follow guidance in Chairman of the Joint Chiefs of Staff Instruction 6211.02C (Reference (ab)) and the Defense IA Security Accreditation Working Group. System owners granted waivers by the DISN/GIG Flag Panel for their information systems shall report approved waivers to the ASD(NII)/DoD CIO within 15 days of approval.

b. For policy compliance issues that have DoD-wide impact or involve multiple DoD Components, Components may submit DoD-wide waiver recommendations through the Director, Identity Assurance and PKI, to the ASD(NII)/DoD CIO. DoD-wide waivers shall be granted only for the minimum length of time required to achieve compliance.

9. COMPLIANCE OVERSIGHT. On behalf of the ASD(NII)/DoD CIO, the Director, Identity Assurance and PKI, will oversee identity authentication compliance efforts including:

a. Establishing and maintaining the DoD guidance and provisions for identity authentication process waivers in coordination with the DISN/GIG Flag Panel as required.

b. Coordinating and monitoring activities or efforts impacting e-authentication that are directed or tasked by the U.S. Cyber Command.

c. Analyzing DoD Component identity authentication compliance information and notifying the DoD Components of shortfalls or duplications of effort.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer
ASD(R&E)	Assistant Secretary of Defense for Research and Engineering
CNSS	Committee on National Security Systems
CRL	certificate revocation list
DAA	designated accrediting authority
DISA	Defense Information Systems Agency
DISN/GIG	Defense Information System Network/Global Information Grid
DoDD	DoD Directive
DoDI	DoD Instruction
FIPS	Federal Information Processing Standards
IA	information assurance
NIST	National Institute of Standards and Technology
NSS	National Security Systems
PACS	physical access control system
PKI	public key infrastructure
SIPRNET	Secret Internet Protocol Router Network
SP	Special Publication
STIG	Security Technical Implementation Guide
USD(I)	Under Secretary of Defense for Intelligence
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
VPN	virtual private network

PART II. DEFINITIONS

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

administrative account. Many operating systems for computers or servers and commercial off-the-shelf software products allow for multiple account types or roles (e.g., User, Power User, System Admin) that have varying levels of privileges. In this Instruction, administrative accounts are considered those accounts that allow elevated privileges. Elevated privileges could

be associated with, but are not limited to, the ability to manipulate or perform system control, monitoring, supervising, end-user administration, administration of common applications, and administration of IA or network devices (e.g., boundary devices, intrusion detection systems, routers and switches).

assurance level. A characteristic associated with a certificate that is an assertion by a Certificate Authority of the degree of confidence that others may reasonably place in the binding of a public key to the identity and privileges asserted in the certificate. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system. Assurance levels are defined in applicable PKI certificate policies.

authenticator. The value or data object (e.g., a password, a biometric template, or a cryptographic key) used to prove the claimant possesses and controls the identity credential. Assertion-based authenticators (e.g., a personal identity number, a password, or a passphrase) are data with no associated physical characteristics or device. Cryptographic-based authenticators are cryptographically generated data or keys (usually only machine readable) carried or stored on a physical device such as the cryptomodule on a smartcard.

certificate. Defined in Reference (y).

CNSS. A committee chaired by the ASD/NII DOD CIO that provides a forum for the discussion of policy issues, and is responsible for setting national-level Information Assurance policies, directives, instructions, operational procedures, guidance, and advisories for U.S. Government departments and agencies for the security of National Security Systems through the CNSS Issuance System. The Department of Defense continues to chair the Committee under the authorities established by NSD-42.

credential service provider. A provider of credentialing services to agencies or companies that do not operate their own credentialing capability.

credential strength. The resistance of the identity credential to forgery or fraud, taking into account the strength of the credential technology used (e.g., resistance to copying or brute force attacks), the identity proofing performed prior to issuance of the identity credential, and the protections incorporated into the system issuing and managing the identity credential. Credential strengths are defined for both unclassified and classified environments.

DAA. Defined in CNSSI 4009 and Reference (o).

DoD-approved PKI. A PKI approved by the ASD(NII)/DoD CIO for use by DoD relying parties. The process for obtaining DoD-approved status is outlined in the DoD External Interoperability Plan (Reference (ac)).

DoD information system. Defined in Reference (b).

DoD mission partners. Federal, State, local, and tribal governments; coalition partners; foreign governments and security forces; international organizations; non-governmental organizations; the private sector; and educational institutes. These partners process electronic transactions with the DoD, or exchange e-mail or other data containing DoD relevant information.

DoD Network. DoD information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

e-authentication level. A set of electronic authentication process requirements that may include stipulations for identity proofing and registration, tokens, token and credential management, authentication protocols, and assertion mechanisms. There are four e-authentication levels defined in Reference (w). This Instruction identifies the types of identity credentials that meet the stipulated requirements for each e-authentication level.

E-authentication level 1 identity credentials require no identity proofing. At this level, the authentication mechanism or protocol provides little or no assurance that the claimant is accessing the protected transaction or data. E-authentication level 1 identity credentials are not approved for use in DoD information systems.

E-authentication level 2 identity credentials provide single factor authentication. There are specific identity proofing, registration, issuance, and credential service provider requirements that must be met for identity credentials to be used in identity authentication processes that are considered e-authentication level 2. These types of identity credentials can be used if issued from a DoD-approved identity credential provider.

E-authentication level 3 identity credentials provide identity authentication using at least two authentication factors. There are specified identity proofing, registration, issuance, and credential service provider requirements that must be met for identity credentials to be used in identity authentication processes that are considered e-authentication level 3. Level 3 authentication processes must use credentials that use one-time password or PKI certificate technology solutions and must include proof of possession of approved types of identity credentials through a cryptographic protocol.

E-authentication level 4 identity credentials provide identity authentication using at least two authentication factors. There are specified identity proofing, registration, issuance, and credential service provider requirements that must be met for identity credentials to be used in identity authentication processes that are considered e-authentication Level 4. Level 4 authentication processes must use credentials that use one-time password or PKI certificate technology solutions and must include proof of possession of an approved hardware cryptographic token through a cryptographic protocol.

hardware token. A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions.

identity authentication. The process of establishing confidence in an entity's (user, process, or device) assertion or claim of an identity that is electronically presented to an information system. In this Instruction, identity authentication refers to electronic authentication to information systems conducted by human users or by non-person entities such as information systems or devices.

identity credential. An object (e.g., a userid or a smartcard) that authoritatively binds an identity (and optionally, additional attributes) to an authenticator (see definition in the Glossary) that is possessed and controlled by a person.

network logon. The process that enables logical access to a fully provisioned DoD network account; an account that provides access to DoD network resources such as domain file shares. Identity authentication and authorization to access a DoD web server or other DoD information system that is hosted on a DoD network or in an approved demilitarized zone is not considered network logon.

NSS. Defined in CNSSI 4009.

PKI. The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates.

relying party. Any entity that uses a digital certificate to identify the creator of digitally signed information, verify the integrity of digitally signed information, or establish confidential communication with the holder of a certificate by relying on the validity of the binding of the subscriber's name to the public key contained in the certificate.

sensitivity level. Sensitivity levels exist for unclassified and classified information. Sensitivity levels indicate the relative importance of any information in an information system that carries the "Sensitive" or "Classified" confidentiality level, as defined and used in Reference (c). Sensitivity levels used in this policy express that information has been evaluated to determine how the risk of unauthorized access or unauthorized dissemination will impact DoD missions or business processes using that data. The reasoning and justifications for why information is considered sensitive (in addition to the information sub-category that the information carries (e.g., For Official Use Only), are key considerations when establishing identity authentication requirements for DoD information systems and networks. Sensitivity levels allow the information owner to evaluate the sensitivity of portions of information within a system. A sensitivity level determination allows an information owner to make an identity credential choice for a user or a group of users that need access to a system because of a particular role or a set of authorization privileges and regardless of the mission assurance category (as defined in Reference (b)) of the system.

smartcard. A credit card-sized token form factor device containing one or more integrated circuits and may employ one or more of the following technologies: magnetic stripe, bar code (linear or two dimensional), non-contact and radio frequency transmitters, integrated circuit chip, biometric information, encryption and authentication information, and photo identification.

web server. An automated information system that manages a website by passing web pages to web browsers over a network. The web server may provide information stored locally on the server or may act as a portal to access information from other linked information systems.