

**Department of the Army
Pamphlet 25-2-7**

**Information Management: Army
Cybersecurity**

Army Information System Privileged Access

**Headquarters
Department of the Army
Washington, DC
8 April 2019**

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25 2 7
Army Information System Privileged Access

This administrative revision, dated 28 October 2022

- o Changes proponency from CIO/G 6 to Deputy Chief of Staff, G 6 (title page).

This new Department of the Army Pamphlet, dated 8 April 2019

- o Establishes requirements for personnel with privileged/elevated access (chap 2).
- o Provides guidance for conducting quarterly reviews of privileged/elevated user accounts in the Army Training and Certification Tracking System (throughout).
- o Corrects the email address (title page).

Information Management: Army Cybersecurity
Army Information System Privileged Access

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:



MARK F. AVERILL
Administrative Assistant to the

History. This publication is an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This pamphlet provides guidance on the Privileged Access Agreement and Non-Disclosure Agreement for personnel who require privileged

access/elevated privileges to Army Information Systems.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Deputy Chief of Staff, G 6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of

the expected benefits and must include

gal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25 30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) via email to usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by paragraph and page number)

Chapter 1

Introduction, page 1

Purpose 1 1, page 1

References and forms 1 2, page 1

Explanation of abbreviations and terms 1 3, page 1

Overview 1 4, page 1

Records management (recordkeeping) requirements 1 5, page 1

Chapter 2

Requirements, page 1

Signing the Privileged Access Agreement 2 1, page 1

Privileged Access Condition 2 2, page 2

Chapter 3

Operational Instructions, page 2

Preparing DD Form 2875 3 1, page 2

Denials for Authorized or Privileged Access and Resubmissions 3 2, page 2

Chapter 4

Oversight and Monitoring, page 2

Oversight 4 1, page 2

Monitoring 4 2, page 2

*This pamphlet supersedes DA Pam 25-2-7, dated 8 April 2019.

Contents—Continued

Chapter 5

Separation of Duties for Privileged Users, *page 3*

Separation of functions 5 1, *page 3*

Dual positions 5 2, *page 3*

Chapter 6

Least Privilege, *page 3*

Assigning minimum system resources 6 1, *page 3*

Operating at assigned duties 6 2, *page 4*

Appendixes

A. References, *page 5*

Glossary

Contents—Continued

Chapter 1 Introduction

1–1. Purpose

This Department of the Army (DA) Pamphlet (Pam) contains amplifying procedures and guidance to AR 25–2 for cybersecurity policy.

1–2. References and forms

See appendix A.

1–3. Explanation of abbreviations and terms

See the glossary.

1–4. Overview

a. Privileged users are those individuals who are authorized to perform security-relevant functions that require elevated access and authorization.

b. Personnel requiring privileges to access and use elevated Information System (IS) accounts will be evaluated by the organizational personnel (for example, system owner, mission/business owner, and/or chief information security officer) responsible for approving such accounts and privileged access. Organizations will define access privileges or other attributes according to account, type of account, or a combination of both. In defining other account attributes, organizations must consider system-related requirements (for example, scheduled maintenance, and system upgrades) and mission/business requirements (for example, time zone differences, customer requirements, and remote access to support travel requirements).

c. Privileged accounts, types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may have a different set of permissions granted to privileged users for domain accounts and for local accounts. This differentiated access should not interfere with the ability to control IS configuration needed to mitigate possible risk.

d. Before authorizing unsupervised privileged access to personnel performing Information Assurance Technical (IAT) Levels I through III functions, managers must ensure that such personnel have, at a minimum, the baseline certification for IAT Level I, in accordance with DODM 8570.01 M.

1–5. Records management (recordkeeping) requirements

The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule Army (RRS A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS A at <https://www.arims.army.mil>. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS A, see DA Pam 25–403 for guidance.

Chapter 2 Requirements

2–1. Signing the Privileged Access Agreement

a. Individuals requiring elevated access to system control, monitoring, administration, criminal investigation, and/or compliance functions must sign a PAA.

b. Individuals seeking privileged access must complete and sign a PAA. Categories and specialties within the cybersecurity workforce that require a PAA include:

(1) Those requiring modification access to the configuration control functions of the IS/network and administration of user accounts, for example.

(2) Those with access to change control parameters (for example, routing tables, path priorities, addresses of routers, multiplexers, and other key IS/network equipment or software).

(3)

Contents—Continued

(4) Those with direct access to operating-system-level functions that could permit system controls to be bypassed or changed.

(5) Those with access and authority to install, configure, monitor, and/or troubleshoot the security monitoring functions of ISs/networks, or in performance of cyber/network defense operations.

2–2. Privileged Access Condition

As a condition of privileged access to any IS, personnel performing Cybersecurity functions described DOD 8570.01 M must satisfy both preparatory and sustaining DOD Cybersecurity training and certification requirements.

Chapter 3 Operational Instructions

3–1. Preparing DD Form 2875

- a. Request privileged access using DD Form 2875 (System Authorization Access Request (SAAR)).
- b. The Information System Security Manager (ISSM) or Information System Security Officer (ISSO) who oversees the local cybersecurity program will authorize or deny requests for privileged access before forwarding to the Network Enterprise Center (NEC) or designated service provider.
- c. The ISSM/ISSO/NEC/designated service provider ensures data ownership and responsibilities are established for each IS, to include accountability, access, and special handling requirements.
- d. Document justification for access in block 13 on DD Form 2875. The Information Assurance Officer (IAO) or appointee will sign in block 22. The IAO or appointee will be the individual responsible for approving access to the system being requested. This person is usually referred to as the Government ISSM/ISSO Block 21 is not a require-

g and Certification Tracking System (ATCTS) profile. The ISSM/ISSO usually requires the originator (user) to upload the form in their ATCTS profile.

3–2. Denials for Authorized or Privileged Access and Resubmissions

- a. The NEC or designated service provider will annotate the reason for denial and send the DD Form 2875 back to the Government supervisor, ISSM/ISSO, and user for the opportunity to resubmit the request, if applicable.
 - (1) Resubmit access requests using the same process as the original request.
 - (2) The authorizing official (AO) will determine, when not clear and agreed upon, the respective NEC or designated

Command Communications Tasking Order 10 133 (Protection of Classified Information on Department of Defense Secret Internet Protocol Router Network (SIPRNET)), AOs will designate authorized personnel responsible for con-
PRNET for the organizations within their area of responsibility.

b. Escalate disagreements regarding enterprise and provider-managed user accounts to the director of the NEC/service provider. For other user accounts, escalate disagreements to the appointed ISSM/ISSO.

c. The final arbiter of any disagreement concerning authorization or denial of privileged access will be the appointed AO.

Chapter 4 Oversight and Monitoring

4–1. Oversight

a. The need for assigned user privileges may change over time, reflecting changes in organizational mission/business functions, environments of operation, technologies, and/or threat. Periodic review of assigned user privileges is necessary to determine whether the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations will take appropriate corrective actions.

b. Commands and other Army ISSOs and ISSMs will revalidate all users with privileged access on a quarterly basis.

4–2. Monitoring

- a. Quarterly reviews.
 - (1) Conduct quarterly reviews in ATCTS at <https://atc.us.army.mil>.

Contents—Continued

(2) Only personnel with ATCTS management rights can conduct the quarterly review. ATCTS managers are individuals who ISSMs/ISSOs trust to oversee their com
ATCTS managers:

- (a)
- (b) Click on the unit management tab.
- (c) t.
- (3)

(as well as users who were not reviewed from previous quarters) is displayed.

b. Revalidate a user.

- (1) All users with a PAA in their ATCTS profile will be displayed for revalidation.
- (2)
- (3)

cies.

- (4)
- c.

(1) button to save your changes and complete the review.

(2) Upload or update the appropriate appointment letter in ATCTS if the user is not in a technical position, or delete appointment letter if the user is no longer working cybersecurity functions.

(3) Q

ISSM/ISSO will notify the NEC or service provider to remove all users whose PAA was revoked so their elevated privileges can be removed.

d. Commands and other Army ISSOs or ISSMs with privileged users will coordinate with their respective NECs

e. Personnel who are not appropriately qualified within 6 months of assignment to a position or who fail to maintain

NEC and service provider to ensure adherence to this requirement.

Chapter 5 Separation of Duties for Privileged Users

5–1. Separation of functions

Separation of duties addresses the potential for abuse of authorized privileges. Separation of duties includes:

- a. Dividing mission functions and IS support functions among different individuals and/or roles.
- b. Conducting IS support functions with different individuals (for example, system management, programming, configuration management, quality assurance and testing, and network security).

5–2. Dual positions

a. Managers of cybersecurity workforce positions that also perform IAT functions (privileged user) must also obtain the appropriate technical level certification and complete the other IAT level (privileged user) requirements prior to being granted unsupervised privileged access.

b. Application of the principle of separation of duties is required per NIST Special Publication 800 53 Revision 4.

Chapter 6 Least Privilege

6–1. Assigning minimum system resources

Least privilege is based on the principle that a security architecture should be designed so that each entity is granted the minimum system resource and authorization that the entity needs to perform their functions (Committee on National Security Systems Instruction 4009).

a. Security functions include (for example, establishing system accounts, configuring access authorizations (such as, permissions and/or privileges), setting events to be audited, and setting intrusion detection parameters).

b. Security-relevant information includes (for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users).

Contents—Continued

6–2. Operating at assigned duties

a. Organizations will employ least privilege for specific duties and ISs. The principle of least privilege also applies to IS processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions.

b. Reassessment of least privilege and separation of duties. Commands and other Army activities must ensure that role assignments are distinct, and must minimize roles and role assignments that allow root access.

Contents—Continued

Appendix A

References

Section I

Required Publications

AR 25–2

Army Cybersecurity (Cited in para 1 1.)

DOD 8570.01–M

Information Assurance Workforce Improvement Program (Cited in para 1 4d.) (Available at <http://www.esd.whs.mil/dd/>.)

NIST Special Publication 800–53 Revision 4

Security and Privacy Controls for Federal Information systems and Organizations (Cited in para 5 2b.) (Available at <http://csrc.nist.gov/publications/pubssps.html>.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication.

AR 25–1

Army Information Technology

CNSSI 4009

Committee on National Security Systems (CNSS) Glossary

DA Pam 25–1–1

Army Information Technology Implementation Instructions

DA Pam 25–403

Guide to Recordkeeping in the Army

DODD 8140.01

Cyberspace Workforce Management

DODI 8500.01

Cybersecurity

DODI 8510.01

Risk Management Framework (RMF) for DOD Information Technology (IT)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the APD website (<https://www.armypubs.army.mil>). DD forms are available on the Office of the Secretary of Defense website (<http://www.esd.whs.mil/directives/forms>).

DA Form 2028

Recommended Changes to Publications and Blank Forms

DD Form 2875

System Authorization Access Request (SAAR)

Contents—Continued

Glossary

Section I

Abbreviations

AO

authorizing official

APD

Army Publishing Directorate

AR

Army Regulation

ARIMS

Army Records Information Management System

ATCTS

Army Training and Certification Tracking System

CNSS

Committee on National Security Systems

DA

Department of the Army

DD

Department of Defense

DOD

Department of Defense

DODD

Department of Defense Directive

DODI

Department of Defense Instruction

IAO

Information Assurance Officer

IAT

Information Assurance Technical

IS

Information System

ISSM

Information Systems Security Manager

ISSO

Information System Security Officer

NEC

Network Enterprise Center

NIST

National Institute of Standards and Technology

PAA

Privileged Access Agreement

Pam

Pamphlet

SAAR

System Authorization Access Request

Contents—Continued

SIPRNET

Secure Internet Protocol Router Network (SIPRNET)

Section II

Terms

Limited privileged access

Privileged access with limited scope (for example, authority to change user access to data or system resources for a single IS or physically isolated network).

Network environment (computer)

The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks.

On-the-job training

Supervised hands-on training based on specific performance criteria that must be demonstrated to a qualified supervisor. An example of an on-the-

Privileged access

Authorized access that provides a capability to alter the properties, behavior, or control of the IS or network. It includes, but is not limited to, any of the following types of access:

a.

tion of user accounts, and so forth.

b. Access to change control parameters (for example, routing tables, path priorities, and addresses) of router, multiplexers, and other key IS or network equipment or software.

c.

d. Direct access (also called unmediated access) to functions at the operating system level that would permit system controls to be bypassed or changed.

e. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of ISs or networks (for example, network or system analyzers, intrusion detection software, and firewalls) or in performance of cyber or network defense operation.

Privileged user

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Super user

A super user is a network account with privilege levels far beyond those of most user accounts. Such an account may belong to a network or a system administrator.