Department of the Army
Pamphlet 25–2–18

Information Management: Army Cybersecurity

Foreign Personnel Access to Information Systems

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY of CHANGE

DA PAM 25–2–18
Foreign Personnel Access to Information Systems

This administrative revision, dated 28 October 2022—

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

This administrative revision, dated 31 May 2019—

- Corrects the e-mail address (title page).

- This new Department of the Army pamphlet, dated 8 April 2019—

- Identifies the process for granting foreign exchange personnel and representatives of foreign nations access to Army information technology (throughout).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army Pamphlet 25–2–18

Information Management: Army Cybersecurity

Foreign Personnel Access to Information Systems

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

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

Summary. This pamphlet supports AR 25–2 and the Army Cybersecurity Program. This pamphlet identifies the process for granting foreign exchange personnel and representatives of foreign nations, coalitions, or international organizations access to Army information technology.

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 formal review by the activity's senior legal 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

1–1. Purpose
Personnel must meet certain criteria before access is granted to Army information technology (IT). Special attention must be given to the controls that govern foreign exchange personnel and representatives of foreign nations access to Army IT. This pamphlet addresses the requirements to ensure standardized and appropriate access.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. 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
Mission Partners

2–1. General
All personnel with access to Army IT must be appropriately cleared and qualified under the provisions of DODI 5200.02. Access to Army IT is granted to individuals based on need-to-know and according to DODI 8500.01, DODI 5200.46, AR 380–67, and AR 25–2.

2–2. Foreign personnel access to information systems
a. Access by foreign officials (FOs).

(1) To ensure standardized and appropriate access to unclassified networks by FO, cybersecurity personnel will enforce the requirements delineated below. All approved access by FO will be documented in the information system (IS) assess and authorize (A&A) package or tenant security plan, as applicable. Provide each authorized foreign official a .mil address on the unclassified network required for executing his or her foreign official duties as outlined in his or her respective delegation of disclosure authority letter (DDL). For each authorized foreign official, the local area network administrator will place a caveat or marker on the user account for that person identifying them as a foreign official from a specific country. The Defense Manpower Data Center will automatically include the official's citizenship in the official's DOD Enterprise Email (DEE) display name. Additionally, the contact officer will ensure the foreign official goes to the milConnect website (https://milconnect.dmdc.mil) and uses the "edit display name" function (on the Personal Information tab of the milConnect profile) to modify the "Preferred First Name" as follows: Spell out the words "Foreign Official" followed by a hyphen and the spelled out country name of the foreign official (not using an acronym for that country.) In addition, the foreign official will indicate the program category of the foreign official (foreign liaison officer (FLO), Cooperative Program Personnel (CPP), Engineer and Scientist Exchange Program (ESEP), standardization representative (STANREP), or Military Personnel Exchange Program (MPEP)). The required tag for each category of FO would thus read as shown below (replace each hypothetical country name with the appropriate one).

(a) FLO: "Foreign Official-Germany-FLO."
(b) CPP: "Foreign Official-Turkey-CPP."
(c) ESEP: "Foreign Official-Israel-ESEP."
(d) STANREP: "United Kingdom-STANREP."
(e) MPEP: "Foreign Official-Italy-MPEP."
(f) Foreign Attaché (FA): "Foreign Official-Italy-FA."

(2) Limit access of FOs to computers that incorporate and enforce Army-mandated access and auditing controls. Approval to access the non-secure internet protocol router network (NIPRNet) does not equate to authority to exchange data or access systems located on that network. Requirements for access to shared drives, portals, or similar local systems must be verified by the FO's contact officer and specified in the supporting position DDL. Similarly, the designated release or disclosure authority will grant access to the information on ISs to FOs on an as-needed basis in accordance with AR 380–10 and in coordination with the responsible foreign disclosure officer/foreign disclosure.

(3) Contact officers will ensure FOs set their mailbox and webmail profiles so that email signature blocks will be automatically inserted into all emails from FOs. The signature blocks must include the user's full name, position (for example, "Foreign Liaison Officer"), and nationality (for example, "United Kingdom").

(4) If the organization where an FO is certified determines there is a need for the FO to have access to the NIPRNet beyond email and local file server or portal access (for example, an Army Knowledge Online (AKO) account), submit an exception to policy through the information system security manager to the authorizing official (AO), to be forwarded to the Chief Information Officer/G–6 (CIO/G–6) (SAIS–CBA). The approval will become part of the IS record in the Enterprise Mission Assurance Support Service (eMASS) system. This includes individuals granted access prior to the publication of this regulation. Commands will immediately evaluate each case and forward their exception recommendation. The exception will be reviewed by the appropriate Headquarters, Department of the Army program manager and the CIO/G–6 Cybersecurity Directorate, prior to disposition. The exception must include the following information:

(a) Request from the commander that states the need-to-know, tied to the FO's certification and DDL. A copy of the DDL must accompany the exception request will be sent via secret internet protocol router network (SIPRNet).

(b) Statements from the network enterprise center and command's information system security officer (ISSO) stating proper cybersecurity procedures are in place.

(c) The Deputy Chief of Staff (DCS), G–2, Foreign Disclosure Branch will review the exception before final disposition.

(d) Statement from the AO authorizing an exception to policy.

(5) Official access to information residing on an IS or network will be limited to that controlled but unclassified information required to fulfill the terms of certification of the FO provided minimum cybersecurity requirements of this section are met.

(6) Disclosure of classified military information to foreign governments and international organizations is limited and will be in accordance with AR 380–10 and DODD 5230.11.

(7) Organizations that have FLO, CPP, ESEP, STANREP, and MPEPs under the American, British, Canadian, Australian Agreement, Five Eve Support Agreement where the position of the FO and the job function at the organization does not change are allowed to exercise a onetime exception for that position. A new exception request is not required for a replacement FO in that position if the position and responsibilities, as documented in the DDL, remain the same. Administrative personnel assigned in support of the foreign representative listed above will be granted access to NIPRNet email and local file servers only. Access permission for all foreign representatives and administrative personnel will be documented in a DDL.

(8) Authority for approval of account sponsorship requests of AKO portal accounts for FOs shall be retained at the Army command (ACOM), Army service component command (ASCC), direct reporting unit (DRU), and program executive office (PEO) command levels, with no delegation authorized. When given, approval will be for contact officers at ACOM, ASCC, DRU, and PEO levels to sponsor the FO for the AKO account. Contact officers must follow AKO account sponsorship guidance at https://ako.us.army.mil when sponsoring FOs for the AKO portal account.

b. Access by international military students (IMSs) on invitational travel orders who have been vetted and approved for U.S. Army training and professional military education under the provisions of AR 12–15.

(1) To ensure standardized and appropriate access to unclassified networks by IMSs attending resident training or enrolled in the Army Distance Education Program at U.S. Army and Army-managed schools/training, cybersecurity personnel will enforce the requirements delineated below. All approved access by IMS will be documented in the IS A&A package or tenant security plan. The Army will provide each authorized IMS a DEE address on the unclassified network if required for course attendance, and access to network resources that host curricula and materials for the course(s) that they attend in accordance with need-to-know and least-privilege principles. IMS sponsors will coordinate with the Project Office Enterprise Email (in the Program Executive Office Enterprise Information Systems) in order to obtain the student's DEE address that will be placed on the common access card (CAC) certificates. The Defense Manpower Data Center will automatically include the student's citizenship in the student's DEE display name.

(2) Limit access of IMS to computers that incorporate and enforce Army-mandated access and auditing controls. Since IMS have already been vetted and approved to attend specific courses of instruction, there is no additional requirement to process exceptions to policy for access to course material approved for release to the IMS. IMS will

agree to comply with all U.S. military department requirements and are required to sign an acceptable use policy (AUP) user agreement. There is no requirement for background investigations as described since in-country U.S. officials perform a security screening of each student before selection approval.

(3) To prevent inadvertent disclosure of information, IMSs will be identified as IMS in their email display name and automatically inserted signature block. The sponsor (and appropriate school official) will ensure the IMS goes to the milConnect website (https://milconnect.dmdc.mil) and uses the "edit display name" function (on the Personal Information tab of the milConnect profile) to modify the "Preferred First Name" as follows: Put the acronym "IMS," followed by a hyphen and the spelled out country name of the student (not using an acronym for that country), for example "IMS-Germany". The signature blocks must include the user's full name, position (for example, "International Military Student"), and nationality (for example, "United Kingdom").

c. Access by non-U.S. citizens other than FO or IMS (for example, local national hires, foreign national (FN) contractors hired under US contractors, FNs serving in the Army).

(1) Access to sensitive information by a non-U.S. citizen who is not a DOD employee or FO certified to the U.S. Army will only be permitted in accordance with applicable policies (for example, DODD 5230.9, DODD 5230.25) and U.S. statutes (for example, the Arms Export Control Act, 22 USC 2551, et. seq.).

(2) Non-U.S. citizens assigned to DOD IT positions are subject to the investigative requirements as outlined in AR 380–67. Non-U.S. citizens, IMSs, or FOs unable to meet national agency check with inquiries investigation requirements must obtain a favorably adjudicated background investigation in accordance with DODI 5200.02, DODI 5200.46, and AR 380–67 and must meet Homeland Security Presidential Directive (HSPD–12) CAC credentialing requirements prior to being granted general user or elevated user access.

(3) Non-U.S. citizens may hold IT positions under the conditions described in the paragraphs above and if the appointed AO for the system and the data owners approve the assignment requirements in writing and submit as part of the A&A package. The written approval must be on file and provided as an artifact to the A&A package in eMASS, before requesting the required investigation. The required investigation must be completed and favorably adjudicated before authorizing access to DOD systems or networks. Interim access is prohibited.

(4) Authority for approval of account sponsorship, requests, of AKO portal accounts for FNs shall be retained at the Army Component, CIO/G–6, in coordination with the DCS, G–2, with no delegation authorized. Follow AKO account sponsorship guidance at https://ako.us.army.mil for guidance. When given, approval will be for ACOM, ASCC, DRU, and PEO level personnel to sponsor the FN for the AKO account. Sponsors must follow AKO account sponsorship guidance at https://ako.us.army.mil when sponsoring FNs for the AKO portal account.

(5) NIPRNet access policy and procedures for FNs in non-official positions as identified above are as follows:

(a) Components or organizations will maintain records on access including the following information:

(b) Specific mission requirements for foreign access or connection.

(c) Justification for each individual FN.

(d) Confirmation that the minimum-security requirements of this section are enacted, including the user agreement discussed below.

d. CAC and alternate smart card logon token (ASCL) requirements for foreign officials, IMS, and FNs.

(1) CAC is the primary hardware token for NIPRNet logon of eligible Army uniformed, civilian and contractor personnel, and properly vetted foreign officials, IMS, and FNs.

(2) ASCL tokens containing medium-assurance software certificates are approved as an alternative Public Key Infrastructure (PKI) credential to the CAC for logical two-factor authentication to the NIPRNet.

(3) FOs/IMS/FNs and non-U.S. citizens who are eligible to receive a CAC, ASCL, or equivalent token still must meet the requirements defined in policy guidance issued by the DCS, G–2: Interim Policy Guidance for Common Access Card (CAC) Background Vetting for Foreign Nationals, dated 5 October 2010.

e. Access to SIPRNet by FOs/FNs.

(1) Generally, an FO/FN or official representative is not authorized access to the U.S. controlled SIPRNet terminal workspace. If an authorized foreign official or FN working at a U.S. Army site has a requirement for accessing the SIPRNet, the commander will follow the Defense Information Systems Agency's (DISA's) joint instruction that can be found on DISA's SIPRNet website at https://www.ssc.smil.mil. The signature blocks for FOs must include the user's full name, position (for example, "Contractor," "Foreign Liaison Officer"), and nationality (for example, "United Kingdom").

(2) Access to SIPRNet by FOs/FNs: Before authorizing FO/FN access to a specific IS on the SIPRNet, Army Components will ensure the FO/FN receives training on the appropriate cybersecurity policies and procedures and the ISSO possesses the authority to enforce these policies and procedures. Before accessing any system, a FO/FN will sign an AUP agreement that includes—

(a) Acknowledgment of appropriate cybersecurity policies, procedures, and responsibilities.

(b) The consequences of not adhering to cybersecurity procedures and responsibilities.

(c) Identification requirements when dealing with others through oral, written, and electronic communications, such as email.

(d) Department of the Army employees or contractors who are non-U.S. citizens and are direct or indirect hires, currently appointed in cybersecurity positions, may continue in these positions provided they satisfy the provisions of DODI 8500.01, and DOD 5200.2–R; have the commanders approval, are under the supervision of an ISSO who is a U.S. citizen, and are approved in writing by the AO and captured in the A&A package.

(e) FNs assigned into IT positions are subject to the same (or equivalent) vetting as defined in policy guidance issued by the DCS, G–2.

(f) FO/FNs may hold or be authorized access to IT positions provided the required background investigation has been completed and favorably adjudicated.

(g) Additionally, an FN may be assigned to a privileged IT position only after the AO who has purview over the system, and the data owner who owns the information sign a waiver and the assignment has been approved by the CIO/G–6 and added to the A&A package. The approvals will become part of the A&A package in eMASS. The waiver must be signed and placed in the individual's security file before requesting the required background investigation. The required background investigation must be completed and favorably adjudicated before authorizing privileged user access to Army systems/networks.

(h) FNs must not be assigned privileged user positions on an interim basis before a favorable adjudication of the required background investigation. This does not include non-privileged access to unclassified information systems.

(3) FO/FN SIPRNet users will be issued SIPRNet PKI hardware tokens that will be used to authenticate SIPRNet resources.

Appendix A

References

Section I

Required Publications

AR 12–15
Joint Security Cooperation Education and Training (Cited in para 2–2*b*.)

AR 25–2
Army Cybersecurity (Cited on the title page.)

AR 380–10
Foreign Disclosure and Contacts with Foreign Representatives (Cited in para 2–2*a*(2).)

AR 380–67
Personnel Security Program (Cited in para 2–1.)

22 USC 2551
Congressional Statement of Purpose (Cited in para 2–2*c*(1).) (Available at http://uscode.house.gov/.)

Section II

Related Publications

AR 25–30
Army Publishing Program

AR 380–40
Safeguarding and Controlling Communications Security Materiel

CJCSI 5128.01
Mission Partner Environment Executive Steering Committee (MPE ESC) Governance and Management (Available at http://www.jcs.mil/library/cjcs-instructions/.)

DA Pam 25–2–1
Army Cross Domain Solution and Data Transfer Management

DA Pam 25–2–2
Cybersecurity Tools Cybersecurity Tools Unified Capabilities Approved Products List Process

DA Pam 25–2–3
Reuse of Army Computer Hard Disk Drives

DA Pam 25–2–6
Cybersecurity Training and Certification Program

DA Pam 25–2–7
Army Information System Privileged Access

DA Pam 25–2–8
Sanitization of Media

DA Pam 25–2–9
Wireless Security Standards

DA Pam 25–2–11
Cybersecurity Strategy for Programs of Record

DA Pam 25–2–12
Authorizing Official

DA Pam 25–2–13
Army Identity and Access Management and Public Key Infrastructure Implementing Instructions

DA Pam 25–2–14
Risk Management Framework

DA Pam 25–2–16
Communication Security

DA Pam 25–2–17
Incident Reporting

DA Pam 25–2–18
Foreign Personnel Access to Information Systems

Deputy Chief of Staff, G–2: Interim Policy Guidance for Common Access Card (CAC) Background Vetting for Foreign Nationals, dated 5 Oct 2010
Available at http://www.dami.army.pentagon.mil/site/persec/docs/armydirective2014-05hspd-12investigationsan-dadjudications.pdf.

DOD 8570.01–M
Information Assurance Workforce Improvement Program (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5230.9
Clearance of DOD Information for Public Release (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5230.11
Disclosure of Classified Military Information to Foreign Governments and International Organizations (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODD 5230.25
Withholding of Unclassified Technical Data From Public Disclosure (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5000.02
Operation of the Defense Acquisition System (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5200.02
DOD Personnel Security Program (PSP) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 5200.46
DOD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8500.01
Cybersecurity (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

DODI 8510.01
Risk Management Framework (RMF) for DOD Information Technology (IT) (Available at http://www.esd.whs.mil/dd/dod-issuances/.)

HSPD–12
Policy for a Common Identification Standard for Federal Employees and Contractors (Available at https://www.dhs.gov/homeland-security-presidential-directive-12.)

TB 380–41
Security: Procedures for Safeguarding, Accounting, and Supply Control of COMSEC Material

Title 8, Code of Federal Regulations
Aliens and Nationality (Available at http://uscode.house.gov/.)

22 USC 39
Arms Export Control (Available at http://uscode.house.gov/.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil).

DA Form 2028
Recommended Changes to Publications and Blank Forms

Glossary

Section I

Abbreviations

A&A
assess and authorize

ACOM
Army command

AKO
Army Knowledge Online

AO
authorizing official

AR
Army Regulation

ASCC
Army service component command

ASCL
alternate smart card logon

AUP
acceptable use policy

CAC
common access card

CIO/G–6
Chief Information Officer/G–6

CJCSM
Chairman of the Joint Chiefs of Staff manual

CPP
Cooperative Program Personnel

DA Pam
Department of Army Pamphlet

DCS
Deputy Chief of Staff

DDL
delegation of disclosure authority letter

DEE
DOD Enterprise Email

DISA
Defense Information Systems Agency

DOD
Department of Defense

DODD
Department of Defense directive

DODI
Department of Defense instruction

DRU
direct reporting unit

eMASS
Enterprise Mission Assurance Support Service

ESEP
Engineer and Scientist Exchange Program

FA
foreign attaché

FLO
foreign liaison officer

FN
foreign national

FO
foreign official

HSPD
Homeland Security Presidential Directive (Available at https://www.dhs.gov/homeland-security-presidential-directive-12.)

IMS
international military student

IS
information system

ISSO
information system security officer

IT
information technology

MPEP
Military Personnel Exchange Program

NIPRNet
non-secure internet protocol router network

PEO
program executive office

PKI
Public Key Infrastructure

SIPRNet
secure internet protocol router network

STANREP
standardization representative