Defense Health Agency

ADMINISTRATIVE INSTRUCTION

NUMBER 5200.07
May 8, 2023

Director, J-1

SUBJECT: Foreign National Vetting and Network Account Policy

References: See Enclosure 1

1. PURPOSE. This Defense Health Agency-Administrative Instruction (DHA-AI), based on the authority of References (a) and (b), and in accordance with the guidance of References (c) through (w), establishes the Defense Health Agency's (DHA) procedures for the Foreign National Vetting and Network Account Policy (FNVNAP).

2. APPLICABILITY. This DHA-AIAI applies to the DHA Enterprise (components and activities under the authority, direction, and control of the DHA) to include: assigned, attached, allotted, or detailed personnel. The terms "market" or "direct reporting market" includes the Hawaii Market unless otherwise noted in the publication.

3. POLICY IMPLEMENTATION. It is DHA's instruction, pursuant to References (a) through (u), that DHA will allow access to unclassified information and information systems by a foreign national (FN) only in accordance with applicable disclosure policies and when such access cannot cause damage to U.S. national security. The FN must obtain a favorable Tier 1 equivalent background check or higher to address additional service specific requirements in accordance with Reference (g) and detailed in DD Form 2875, "System Authorization Access Request (SAAR)," and must have valid justification for network access and a need to access basis. All FN accounts shall be reviewed annually from the date authorization was granted.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. PROPONENT AND WAIVERS. The proponent of this publication is the Director, Administration and Management (J-1). When Activities are unable to comply with this

publication, the activity may request a waiver that must include a justification, including an analysis of the risk associated with not granting the waiver. The activity director or senior leader will submit the waiver request through their supervisory chain to the Director, J-1to determine if the waiver may be granted by the Director, DHA, or their designee.

7. RELEASABILITY. **Cleared for public release**. This DHA-AIAI is available on the Internet from the Health.mil site at: https://health.mil/Reference-Center/Policies and is also available to authorized users from the DHA SharePoint site at: https://info.health.mil/cos/admin/pubs/SitePages/Home.aspx.

8. EFFECTIVE DATE. This DHA-AI:

a. Is effective upon signature.

b. Will expire 10 years from the date of signature if it has not been reissued or cancelled before this date in accordance with Reference (c).

9. FORMS. DD Form 2875, "System Authorization Access Request (SAAR)" can be found at: https://www.esd.whs.mil/Directives/forms/dd2500_2999/.

CROSLAND.TELITA.1017383040
Digitally signed by CROSLAND.TELITA.1017383040
Date: 2023.05.08 09:40:58 -04'00'

TELITA CROSLAND
LTG, USA
Director

Enclosures
1. References
2. Responsibilities
3. Procedures

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5136.01, "Assistant Secretary of Defense for Health Affairs (ASD(HA))," September 30, 2013, as amended
(b) DoD Directive 5136.13, "Defense Health Agency," September 30, 2013, as amended
(c) DHA-Procedural Instruction 5025.01, "Publication System," April 1, 2022
(d) United States Code, Title 10, Section 1073c
(e) DoD Manual 5200.02, "Procedures for the DoD Personnel Security Program (PSP)," April 3, 2017, as amended
(f) Chairman of the Joint Chiefs of Staff Instruction 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)," February 9, 2011, as amended
(g) DoD Instruction 5200.46, "DoD Investigative and Adjudicative Guidance for Issuing the Common Access Card (CAC)," September 9, 2014, as amended
(h) Office of Personal Management Memorandum, "Credentialing Standards Procedures for Issuing Personal Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for Personal Identity Verification Credentials," December 15, 2020
(i) DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended
(j) Office of Personnel Management Memorandum, "Frequently Asked Questions (FAQs) for Credentialing Standards Procedures for Issuing Personnel Identity Verification Cards under HSPD-12 and New Requirement for Suspension or Revocation of Eligibility for PIV Credentials," December 15, 2020
(k) Office of Personnel Management Memorandum, "Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12," July 31, 2008
(l) Office of Personnel Management Memorandum, "Guidance on Executive Branch-Wide Requirements for Issuing Personal Identify Verification (PIV) Credentials and Suspension Mechanism," March 2, 2016, as clarified by Reference (j)
(m) DHA-Administrative Instruction 5015.01, "Records Management Program," February 6, 2020
(n) DoD Instruction 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," May 24, 2011
(o) DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6, 2020
(p) Regulation (EU) 2016/679 of the European Parliament and the Council, "General Data Protection Regulation," April 27, 2016
(q) National Disclosure Policy (NDP-1), 1 October 1988, "National Disclosure Policy and Procedures for Disclosure of Classified Military Information to Foreign Governments and International Organizations"
(r) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(s) DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005
(t) DoD Instruction 5530.03, "International Agreements," December 4, 2019

(u) Federal Investigation Notice No. 15-03 "Implementation of Federal Investigative Standards for Tier 1 and Tier 2 Investigations," November 4, 2014.
(v) DoD Instruction 8520.03 "Identity Authentication for Information Systems"
(w) "International Program Security Handbook" Office of the Deputy to the Under Secretary of Defense (Policy) for Policy Support 1993
(x) CAC IAW DTM 08-003, "Next Generation Common Access Card (CAC) Implementation Guidance"
(y) DoD Instruction 1000.13 "Identification (ID) Cards for Members of the Uniformed Services, Their Dependents, and Other Eligible Individuals" December 14, 2017
(z) DoD 8570.01-M "Information Assurance Workforce Improvement Program" December 19, 2005 Assistant Secretary of Defense for Network and Information Integration/Department of Defense Chief Information Officer
(aa) Section 2767 of title 22, United States Code, as amended
(ab) Section 2350(a), title 10, United States Code, as amended
(ac) DoD Manual 5200.01 V1-3 "DoD Information Security Program" February 24, 2012

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DHA. The Director, DHA, through this Instruction, establishes the FNVNAP to be managed by the Chief, Administration Security Division (ASD) and ensure the necessary resources are available to perform investigations, provide vetting services, and maintain accountability for foreign national access to unclassified systems.

2. DIRECTOR, J-1. The Director, J-1 must authorize and ensure implementation of the DHA FNVNAP and provide oversight of the program once established.

3. PERSONNEL EXECUTIVE OFFICER MEDICAL SYSTEMS/CHIEF INFORMATION OFFICER (J-6). The Personnel Executive Officer Medical Systems/Chief Information Officer (J-6) or designee appointed in writing will approve or deny all complete FN account request packages for FNs and assume the risk on behalf of the Agency for granting all FN accounts.

4. CHIEF, ADMINISTRATION SECURITY (ASD). The Chief, ASD, J1, or their designee (established by written delegation with the authority to execute) will approve and implement all agency-wide and/or site-specific guidance regarding the execution of the DHA FNVNAP procedures, processes, and guidelines, in addition to overseeing the management of and providing the oversight for the FNVNAP.

a. Designate, in writing, as Principal Disclosure Authority (PDA), to appoint a Designated Disclosure Authority in order to implement this instruction within their cognizance and establish written procedures and processes to approve or deny requests for visits and assignments of foreign nationals covered by this instruction.

b. Process and record the decisions on Request Foreign Visit (RFV) authorizations involving access by foreign nationals to classified information and CUI.

c. Ensure that all assignments of foreign nationals are in accordance with legally binding international agreements and prepared according to this instruction.

d. Ensure the contents of all specialized training in foreign disclosure and security requirements for international programs are coordinated with the Deputy Under Secretary of Defense for Technology Security Policy and Counter-Proliferation (DUSD(TSP&CP)) pursuant to reference (s).

e. Forward any inquiries on the application of this Instruction to the Office of the DUSD(TSP&CP) reference (s).

5. DHA INFORMATION SECURITY PROGRAM MANAGER. The DHA Information Security Program Manager will oversee all functions in this manual and report directly to Chief, ASD, J1.

6. DHA FOREIGN DISCLOSURE OFFICER (DHA FDO). The DHA FDO shall:

a. Be designated in writing as the Designated Disclosure Authority by the Chief, ASD, J1 to implement this instruction within DHA cognizance and assume all duties outlined in enclosure 2 (4.a – e). Manage day-to-day disclosure activity for DHA and enterprise.

b. Ensure that all assignments of foreign nationals and account accesses are in accordance with legally binding international agreements and prepared according to this instruction.

c. Will process DD Form 2875 (SAAR form), Section III, in accordance with this manual and Foreign National Security Certificates.

7. DHA INFORMATION SYSTEM OFFICER/MANAGER. The DHA Information System Officer/Manager at each level of the Enterprise, for their given DHA Component, will provision and deprovision the approved FN accounts in accordance with Reference (v) through the DHA Component information systems owner/manager.

8. DIRECTORS OR ASSISTANT DIRECTORS, DHA COMPONENTS. The Directors or Assistant Directors, DHA Components, or their designee (established by written delegation with the authority to execute) must:

a. Coordinate with servicing DHA security office and the Host Nation's Work Council or other similar authority through the local Security Manager, to ensure vetting has met the equivalent criteria of a Tier 1 background investigation or higher in accordance with Section 27.e.(6) of Enclosure C of Reference (f).

b. Ensure DHA Components without a Security Manager have their vetting processes managed by the DHA HQ Personnel Security Office.

c. Provide DD Form 2875 to the DHA EAD via email at dha.dd2875@health.mil or via an identified successor case management system.

d. Notify the Host Nation's Work Council or other similar authority and the local DHA Security Office if a background investigation is no longer determined favorable and requires deprovisioning as soon as possible.

e. Review and verify the need for access for all FN accounts with frequency based on the Host Nation's Embassy policy.

f. Maintain all account request documentation in a DHA-approved records management system with the guidance of Reference (m).

g. Ensure that an alternative facility access identity credential may be issued, as needed, based upon an appropriate risk determination in accordance with Reference (h) through (l).

9. DHA COMPONENT INFORMATION SYSTEMS SECURITY MANAGER (ISSM)/INFORMATION SYSTEMS SECURITY OFFICER (ISSO). The DHA Component ISSM or ISSO will:

a. Maintain security groups for FN accounts ensuring limited access to approved FN systems.

b. Works with DHA information security program manager to verify the enforcement of CUI, the limited access requirement, and report all access beyond the approved systems by FN account holders to the DHA Information System Security Manager/Officer (ISSM or ISSO), the Foreign Security Manager, and the DHA Component Director.

c. Ensure workstations used by FNs use a naming convention that identifies the workstations as limited FN access only, following DHA IT naming convention guidance.

d. Ensure established monitoring systems and firewalls are in place for inbound and outbound communication traffic to detect attacks and indicators of potential attacks.

e. Review all completed account requests and approve or deny the requests.

f. Audit all FN accounts (from date access was granted) to maintain compliance with References (v).

10. DHA COMPONENT CONTACT OFFICER. The DHA Component Contact Officer shall:

a. Be knowledgeable in policies in reference (s) and shall be designated for foreign nationals and responsible for their component(s) foreign nationals assigned.

b. A government or military employee designated, in writing, to oversee and control all contacts, request for information, consultations, access, and other activities of the foreign nationals who are assigned to their DHA component.

ENCLOSURE 3

PROCEDURES

1. INVESTIGATIVE REQUIREMENTS.

a. At Foreign Locations. In accordance with Reference (g):

(1) DHA Components must initiate and ensure completion of a background investigation before applying the credentialing standards to a non-U.S. national at a foreign location. The background investigation must be favorably adjudicated before a common access card (CAC) can be issued to a non-U.S. national at a foreign location. Non-U.S. nationals at foreign locations are not eligible to receive a CAC on an interim basis even if their background investigation is deemed favorably adjudicated. The type of background investigation may vary based on standing reciprocity treaties concerning identity assurance and information exchanges that exist between the U.S. and its allies or agency agreements with the host country.

(2) The investigation of a non-U.S. national at a foreign location must be consistent with a Tier 1 equivalent background check; which covers all investigative requirements of a National Agency Check with Inquires, to include a fingerprint check against the Federal Bureau of Investigation (FBI) criminal history database, an FBI investigations files (name check) search, and a name check against the terrorist screening database.

(3) In the event that a FN is approved for network access, but the local government policy prohibits CAC issuance, a Non-classified Internet Protocol Router Network (NIPRNet) Enterprise Alternate Token can be issued through the NIPRNet Enterprise Alternate Token System (NEATS), in accordance with Enclosure 3, Paragraph 1.d of Reference (n). NEATS provides an enterprise capability for issuing and managing Alternate Tokens on NIPRNet including person use cases for those not eligible to receive or use a CAC. An example system that would appropriately fulfill this requirement would be the DoD NEATS, which can be found at the following link: https://intelshare.intelink.gov/sites/dha-hit-csd/cso/pki/tokens/Pages/NEATS.aspx.

b. At U.S.-Based Locations and in U.S. Territories (other than American Samoa and Commonwealth of the Northern Mariana Islands):

(1) Individuals who are non-U.S. nationals in the United States or U.S. territories for three years or more must have a Tier 1 equivalent investigation initiated after employment authorization is appropriately verified.

(2) FNs who have been in the CONUS or U.S. territory for fewer than three years do not meet the investigative requirements for CAC issuance. DHA may delay the background investigation of a FNs until the individual has been in the CONUS or U.S. territory for at least three years. In the event of such a delay, an alternative facility access identity credential may be issued at the discretion of the DHA Component Director, Assistant Director, or their designee, as

appropriate based on a risk determination, and in accordance with References (h) through (l). However, at locations where DHA is a tenant, and not exercising direction, authority, and control over the location, DHA will not allow reciprocity for non-DHA issued alternate credentials as per Reference (h).

2. INVESTIGATION AND VERIFICATION

a. Tier 1 Equivalent Background Investigation. Tier 1 is the basic and minimum investigation required on all new federal and contract employees, volunteers, and students. It consists of a National Agency Check with written inquiries and searches of records covering specific areas of a person's background during the past five years. Those inquiries are sent to current and past employers, schools attended, references, and foreign law enforcement authorities, per Chapter V, Article 45, Section 1 of Reference (p). If an investigation that is equivalent to a Tier 1 investigation cannot be performed, an alternative facility access identity card may be issued at the discretion of the following in accordance with Enclosure C, para. 27.e of Reference (f). The Office of Personnel Management, in Reference (j), has determined the following list to be equivalent to a Tier 1 for the purpose of FN accounts:

(1) Department of State Chief of Mission Authority.

(2) DHA Component Director and/or their designee, as appropriate, based on a risk determination.

b. Verification is required, in accordance with Section 3.1.c and Section 6 of Reference (e), with the following U.S. systems or FN system equivalent:

(1) FBI National Crime Information Center Check must be completed before an identity card is issued.

(2) Terrorist Screening Database.

(3) U.S. Citizenship and Immigration Services Check against Electronic Immigration Verification System or Systematic Alien verification for Entitlements.

(4) Defense Manpower Data Center: Defense Biometric Identification System.

(5) Any additional checks the DHA Component Director determines are necessary.

(6) Any standards, criteria, and guidelines required for system access to Controlled Unclassified Information (CUI), including but not limited to:

(a) CUI Annual Certification Training,

(b) Cyber Awareness Training,

(c) DHA Account User Agreement, and;

(d) Annual HIPAA/Privacy Act Training.

c. For FN records check which results in an original, certified, and favorable result from foreign law enforcement agency (or other appropriate government agency):

(1) Hard copies of records, in English (if English language reports cannot be provided, translation services must be coordinated with local authorities as appropriate), shall be maintained by the DHA Component Director.

(2) The DHA Component Director must provide notification to the Component Security Manager in the event of a change in status of a FN within one hour.

(3) In all cases, as soon as Personal Identity Verification (PIV) credential access is no longer needed, the DHA Component Director, Assistant Director, or their designee will notify the DHA Component Information System Manager/Owner and access shall be withdrawn for the Personal Identity Verification and credentialing access to network data bases must be revoked and terminated.

d. System Account Request Required Documentation. All current forms and documents required for FN accounts for NIPRNet are listed below:

(1) Cyber Awareness Training Certificate (valid if taken within the same year).

(2) SAAR form

(3) Director, J-1, memorandum indicating results of background check (three years or more)

(4) Designated of Disclosure Authority Letter (DDL) through SIPR.

(5) Security Assurance

(6) Foreign Visit Request (FVR) submitted through DoD Foreign Visits System (FVS).

e. Bilateral or multinational agreements or programs often provide the opportunity for hosting foreign nationals or assigning such personnel to DHA organizations as Foreign Liaison Officers (FLO), exchange personnel, or cooperative program personnel. Reference (s) establishes the guidelines by which visits and assignments to DoD organizations by foreign nationals are conducted. As such, all official international visits or assignments to DHA organizations will comply with the cited policy and with the guidance contained herein.

g. An official foreign visit is a visit to a DHA organization by a foreign national who is sponsored by their foreign government or international organization to perform official duties approved by the government or organization. Therefore, it is important that such visits are

processed, planned, and conducted in a professional, respectful and policy-compliant manner. DHA personnel must be careful not to make or insinuate the making of a commitment to disclose or transfer Classified Military Information, CUI, controlled technology or technical data, or defense-related articles and/or services unless they have been granted such authority (in writing) by an appropriately authorized official.

h. CMI, CUI, controlled technology or technical data, or defense-related articles and/or services is not to be disclosed to a foreign visitor (including liaison officers and exchange personnel) unless the appropriate Principal Disclosure Authority (PDA) or Designated Disclosure Authority (DDA) has authorized the disclosure and has received security assurance from the visitor's foreign government in accordance with References (r) and (s). CMI, CUI, controlled technology or technical data, or defense-related articles and/or services may only be transferred via Government-to-Government channels and only when the visit request, or terms of certification for FLOs, specifically states the individual may assume custody on behalf of the foreign government and the visitor has the necessary courier documentation. A receipt must be obtained for all materials provided to a foreign representative, regardless of classification level.

i. Unless exempted under the provisions of Reference (s), RFVs to DHA organizations in the continental United States (CONUS) by foreign nationals representing a foreign government or international organization will be processed through the DoD Foreign Visit System (FVS), a component of the SPAN. The DHA-FVO, serving as the Agency's FVO, will review, coordinate, and process proposed RFVs to DHA organizations.

j. Unless specifically stated in the visit authorization, foreign nationals are not authorized to request documentary information (CMI, CUI or other protected information) directly from the visit host. Requests for documentary information must be submitted through the visitor's embassy and transferred via Government-to-Government channels.

3. TYPES OF FOREIGN VISITS

a. Official Visits. In accordance with Reference (w), an official foreign visit occurs when a foreign national is sponsored by his or her government or by an international organization and visits a DoD Component or cleared contractor facility to perform official business approved by the government or the organization. Listed below are the types of official visits.

(1) One-time Visits. "One-time" visits are single, short-term visits to a single DHA facility for a specific purpose. A one-time visit will not normally exceed 30 days and normally requires at least 21 workdays for processing by the Defense Visit Office.

(2) Emergency Visits. Emergency visits are one-time, short notice visits and are identified as such in the RFV. Emergency visit requests are limited to situations in which failure to conduct the visit will jeopardize an official government project, program, or contract.

(a) The requestor should coordinate the emergency visit in advance with the person to be visited and ensure the complete name, grade or position, address and telephone number of the person and a knowledgeable foreign government point of contact (POC) are provided in the

visit request. In addition, the RFV will identify the applicable contract, agreement, or program and a justification for submission of the emergency request. Emergency RFVs will not be accepted less than one full working day prior to the requested visit.

(b) Emergency visit requests will not be submitted to circumvent routine visit approval procedures. If circumvention is suspected, report the situation to the DHA FDO so appropriate action can be taken to preclude such submissions in the future.

(3) Recurring Visits. A recurring visit constitutes multiple visits to a single DHA office on an intermittent basis in support of on-going international agreements, contracts, programs, or export authorizations when the information/material to be released has been defined and approved for release by the applicable government disclosure authority. A recurring visit will not exceed one year's duration. Generally, except for emergency visits, the pertinent foreign office or visitor(s) should give the host activity a reasonable amount of notice of the date and time of any proposed visit. DHA organizations may refuse a visit if the visitor arrives without appropriate advance notice.

(4) Extended Visits. An extended visit is a long-term visit to a single DHA office/facility on an extended basis in support of on-going international agreements, contracts, or programs. Such visits are normally used to certify national representatives and other FLOs stationed at their embassies who are authorized to conduct business with DoD components. These visits also document foreign assignments to DoD Components under the terms of relevant international agreements. Extended visit authorizations are designed for use when a foreign representative is required to be in continuous contact with a DoD Component in support of government contracts, joint programs or other international agreements.

(5) Unofficial Visits. An unofficial visit is any occasion when a foreign national who is not sponsored by his or her government or by an international organization visit for unofficial purposes or to conduct business which will entail access to information in the public domain. Examples of unofficial visits include courtesy calls, public tours, commercial-related transactions, and/or routine coordination visits OCONUS where the disclosure of CMI or CUI will not take place. Access to DHA organizations by such persons will be reviewed on a case-by-case basis and if approved, managed the same as visits by U.S. citizens without a security clearance.

b. Invitational Visits.

(1) Visit invitations extended by DHA to foreign representatives of an official nature will comply with the requirements of Reference (s) and other applicable statutes and policies.

(2) Directors will notify the DHA FVO of planned invitational visits in order to ensure appropriate security protocols are established and to ensure documentation in the DoD FVS in accordance with Reference (s), paragraph 4.8.

(3) Unless otherwise approved in writing by the Director, DHA and the responsible DHA FDO, invitational visits will not involve the disclosure of CMI, CUI, or other protected information.

c. Visit Amendments. The requesting embassy may amend an official RFV. Amendments are limited to the date(s) of the visit and/or the names of the visitors. If any other element of the RFV requires an amendment, a new visit request must be submitted. Emergency visits may not be amended.

4. PROCESSING REQUESTS FOR VISITS

a. Official visits by a representative(s) of a foreign government or international organization to DoD organizations will be processed in accordance with Reference (s) and will coincide with network access.

b. Upon receipt of the RFV, the DHA FDO (or designated representative) will coordinate the request with the knowledgeable DHA point of contact (identified in the RFV), the responsible DHA Director (or designated representative), and the contact officer or designee, designated to supervise the foreign national.

c. At a minimum, the FVO will provide the following information (from the RFV) during the coordination process:

(1) Dates, times and exact location of the proposed visit;

(2) Country submitting the request; and

(3) Names of foreign representatives to participate in the visit.

5. FOREIGN PERSONNEL ACCESS TO INFORMATION SYSTEMS

a. Access by foreign officials (FO).

(1) The DHA FDO will work with ISSO/ISSM's and contact officer to authorize access to DHA information systems or CUI on a need-to-know basis for official duties by foreign nationals (e.g., DOD foreign national employees (direct and indirect hires) or military, civilian, or contract employees of foreign governments serving with DOD).

(2) Authorize access to U.S. classified information systems and workstations as specifically authorized if the classification level that has been delegated for the subject matter category and specific nation or organization as described in annex a of reference (q) or Delegation of Disclosure Authority Letter.

(3) DoD Rapids/CAC office will issue eligible foreign nationals a per reference (x). A CAC may be issued when the non-U.S. person meets the requirements of paragraph 3.a.(3) and reference (y). Visiting and assigned foreign nationals must possess a visit status and security assurance that has been confirmed, documented, and processed in accordance with international agreements and Reference (s)

(4) DHA-FDO and ISSM/ISSO will ensure a foreign national employee covered by a Status of Forces Agreement (SOFA) with privileged information systems access for unclassified information security systems receives a host-nation personnel security investigation that is the equivalent of the U.S. investigative level per reference (e) and (v).

(5) ISSM/ISSO will work with DHA-FVO to acquire all required documentation from this instruction and will approve foreign national access to unclassified information systems (e.g., NIPRNET).

(6) ISSM/ISSO may approve foreign national access to U.S. classified information systems as specifically authorize under Information Sharing guidance outlined in changes to NDP-1.

(7) ISSO/ISSM shall notify the DISA connection approval office when foreign nationals are authorized access to enclaves connected to the SIPRNET.

(8) The Chief, ASD, J1 or their designee shall ensure DHA designated official(s) are authorized to grant a foreign national access are designated.

(9) The DHA-FDO will identify sponsors for all approved information systems access by foreign nationals and provide the information to the Authorizing Official (i.e., Designated Accrediting Authorities, DAA) with appropriate control measures identified to protect information.

(10) The DHA-FDO will ensure foreign national employees meet the same or equivalent requirements as all DOD authorized users (i.e., military and DoD government civilian and contract employees) for access to DoD information systems and networks.

(11) DHA-FDO will ensure a foreign national employee covered by a SOFA with privileged (IA Management) access for unclassified information systems receives a host-nation personnel security investigation that is the equivalent of the U.S. investigative level reference (e) and (v).

b. The Authorizing Official (i.e., Designated Accrediting Authorities, DAA) shall perform functions below and outlined in reference (z):

(1) Ensure system certification and accreditation documentation is updated to reflect foreign national access.

(2) Ensure security measures employed adhere to the DoD, DHA, and local IA and system security guidance and procedures.

(3) Ensure accountability is maintained through audit trails of all actions taken by foreign nationals within ISS.

(4) Ensure foreign users sign a user agreement and receive initial IA awareness training prior to gaining access. User agreement will outline DOD and local information systems security policies and procedures and consequences of misuse.

(5) Ensure the Information Systems Security Managers and Information Systems Security Officer are given authority to enforce policies and revoke access if deemed necessary

(6) Ensure that the foreign national is identified when dealing with others through written and electronic communications, such as e-mail.

(7) Ensure the following minimum controls are implemented for foreign nationals per the section below:

(8) Ensure workstations accessed by foreign nationals can be logically grouped and managed (e.g., virtual LAN, static IP address or Dynamic Host Configuration Protocol (DHCP)).

(9) Disable modem ports, CD drives, USB ports, and unused network interface car s (NICs).

(10) Port security shall be enabled in accordance with DOD Access Control STIG.

(11) Establish Active Directory Organizational Unit specifically for foreign nationals.

(12) Prevent foreign nationals from accessing U.S.-only public folders.

(13) 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). 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).

(14) 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. Additionally, the contact officer will ensure the foreign officials goes to the milConnect website (https://milconnect.dmdc.osd.mil/milconnect/) 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 foreign official (foreign liaison officer (FLO), Cooperative Program Personnel (CPP), Engineering 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-Italy-MPEP."

(d) STANREP: "United Kingdom-STANREP."

I MPEP: "Foreign Official-Italy-MPEP."

(15) Limited access of FOs to computers that incorporate and enforce DHA-mandated access and auditing controls. Approval to access systems located on the network. Requirements for access to shared drives, portals, or similar local systems must be verified by the FO's contact officer and specific 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 this AI and in coordination with the responsible foreign disclosure officer/foreign disclosure.

(16) 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 (e.g., "Foreign Liaison Officer"), and nationality (e.g., "United Kingdom).

c. Foreign National Access to U.S.-Only Workstations and Network Equipment.

(1) Maintain strict U.S. control of U.S.-only workstations and network equipment at all times.

(2) Group U.S.-only workstations together in a U.S.-controlled workstation space when workstations are in workspaces physically accessible by foreign nationals (such as combined operations centers).

(3) If the grouping of U.S.-only workstations at a site is not operationally possible, the following steps shall be taken by the responsible level of the enterprise:

(4) The DHA HQ may authorize an exception at the site, in writing, to stating operational reasons for exception, and maintain the record of exception.

(5) Develop, publish, and maintain specific site written procedures on security measures to safeguard U.S.-only classified workstations.

(6) Ensure that U.S. personnel are briefed and enforce security measures.

d. Announce presence. If a foreign national is permitted access to U.S.-controlled workstation space, the individual must be announced, must wear a badge clearly identifying him or her as a foreign national, and must be escorted at all times. In addition, a warning light must be activated if available and screens must be covered or blanked.

(1) If the foreign national is permitted to view the screen, U.S. personnel must ensure:

(2) Information is releasable in accordance with DHA HQ guidance and shall be consistent with references (q); DODD 5230.11 and (ab); DODD 5230.11; 5200.01 V1-3.

(3) Check with DHA HQ FDO to ensure foreign national has security clearances granted by their government at a level equal to that of the classified information involved and an official need-to-know.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CAC	Common Access Card
CMI	Classified Military Information
CONUS	Continental United States
CUI	Controlled Unclassified Information
DDA	Designated Disclosure Authority
DDL	Delegation of Disclosure Authority Letter
DHA	Defense Health Agency
DHA-AI	Defense Health Agency-Administrative Instruction
DHA FDO	Defense Health Agency Foreign Disclosure Officer
FBI	Federal Bureau of Investigation
FDO	Foreign Disclosure Officer
FN	Foreign National
FNVNAP	Foreign National Vetting and Network Account Policy
FVS	Foreign Visits System
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
IT	Information technology
NEATS	Non-classified Internet Protocol Router Network Enterprise Alternate Token System
NIPRNet	Non-classified Internet Protocol Router Network
PDA	Principal Disclosure Authority
RFV	Request Foreign Visit

PART II DEFINITIONS

Assignment. The placement of a military or civilian official of a foreign defense establishment on the premises of a DoD Component or cleared contractor facility.

Contact Officer. A government or military employee designated, in writing, to oversee and control all contacts, requests for information, consultations, access and other activities of foreign nationals who are assigned to DoD component or subordinate organization.

Cooperative Program. For the purposes of this administrative instruction, programs that comprise one or more specific cooperative projects with a foreign government or international organization whose arrangements are defined in a written agreement between the parties covering research, development, test, and evaluation, joint production (including follow-on support) under 22 U.S.C. 2767 reference (aa), or a cooperative research and development program defined in a written agreement with NATO and major non-NATO allies under 10 U.S.C. 2350a reference (ab).

Defense Personnel Exchange Program. (DPEP). A program authorized by reference (o) where military and civilian personnel of the Department of Defense and the defense ministries/departments and/or armed services of foreign governments occupy positions with and perform functions for a host organization to promote current or future international programs, greater mutual understanding, and interoperability with allies and coalition partners. DPEP is composed of the MPEP, the APEP, the ESEP, and the DIPEP.

Delegation of Disclosure Authority Letter. (DDL). A letter issued by the appropriate PDA or Designated Disclosure Authority describing classification levels, categories, scope, and limitations related to information under a DoD Component's disclosure jurisdiction that may be disclosed to specific foreign governments or their nationals for a specified purpose.

Designated Disclosure Authority. An official, designated by the Head of a DoD Component or by the DoD Component's PDA, who has been delegated disclosure authority in accordance with reference (h), to control disclosures by subordinate commands or staff elements of classified information to foreign governments and their nationals and to international organizations.

Foreign Exchange Personnel. Military or civilian officials of a foreign defense establishment who are assigned to a DoD Component in accordance with the terms of a personnel exchange agreement and who perform prescribed duties for the DoD Components.

Foreign Liaison Officer (FLO). Military or civilian officials of a foreign defense establishment who are authorized by their government or an international organization, and certified by a DoD Component, to act as an official representative of that government or organization in dealing with the DoD Components.

Foreign National. Any employee, contractor, volunteer, or student, whose citizenship or national allegiance belongs to a foreign government or non-governmental organization.

International Visits Program (IVP). The program established to process visits and assignments of foreign nationals to the DoD Components and cleared contractor facilities. It is designed to ensure that classified information and CUI to be disclosed to such visitors has been properly authorized for disclosure to their governments, to ensure that the requesting foreign government provides a Security Assurance for the proposed visitor when classified information is involved in the visit or assignment, and to facilitate administrative arrangements (e.g., date, time, and place) for the visit or assignment.

NACI. The National Agency Check with Inquiries that make up the basic and minimum investigation required on all Federal employees. The NACI consists of a national agency check with written inquiries and searches or records covering specific areas of a person's background covering a minimum of the past five years of history. OPM is conducting "Tier 1" Investigations in lieu of former National Agency Check and Inquires.

Principal Disclosure Authority (PDA). A senior official appointed by the Head of a DoD Component as the principal disclosure official for that Component.

Security Assurance. For the purpose of this Directive, a written confirmation by a responsible foreign government official that the proposed visitor possesses the requisite security clearance and need-to-know for the classified information and CUI to be released during the visit. The Security Assurance certifies that the recipient government will protect the information in accordance with the international agreement between the United States and the foreign government.

Security Policy Automation Network. An automated system that assists DoD decision-makers and analysts in reviewing, coordinating, reaching decisions, and maintaining records on proposals to release classified information and technology to other nations and international organizations.

Technology Control Plan. A detailed plan to control access by foreign national employees and by foreign national visitors on an extended visit authorization at a DoD cleared contractor facility.

Tier 1. Investigation for positions designated as low-risk, non-sensitive. It is also the minimum level of investigation for final credentialing determination for physical and logical access.