BY ORDER OF THE COMMANDER,
PACIFIC AIR FORCES

AIR FORCE INSTRUCTION 33-202

PACIFIC AIR FORCES COMMAND
Supplement 1

12 FEBRUARY 2002

Communications and Information

COMPUTER SECURITY

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://afpubs.hq.af.mil.**

OPR: HQ PACAF/SCI
(Capt Kelly Roth, TSgt Eric Wolfe)

Certified by: HQ PACAF/SCI
(Lt Col Nurbert A. Hughes)
Pages: 26
Distribution: F

This supplement applies to all personnel that use, administer or manage automated information systems, business-applications, or computer networks in PACAF. It does not apply to the Air National Guard (ANG) or the Air Force Reserve Command (AFRC) units.

Item: Foreign National Access. All Foreign national positions and personnel currently in place (excluding summer hires, temporary hires, volunteers for employment to last 180 days or less, and exercise participants) have one year from the date of this document to fully comply with its requirements. All new hires/positions that occur after 1 Jun 02 must comply immediately with this supplement. All summer hires, temporary hires, volunteers for employment to last 180 days or less, and exercise participants must comply immediately.

AFI 33-202, 30 August 2001, is supplemented as follows:

2.9. The PACAF Command Information Assurance Division, HQ PACAF/SCI, implements and oversees the MAJCOM COMPUSEC, COMSEC, EMSEC, and Information Assurance Awareness programs. HQ PACAF/SCI provides policy, guidance and supplements for PACAF Information Assurance (IA). HQ PACAF/SCI distributes copies of command supplements to HQ AFCA.

2.9.1.4. The PACAF Network Operations and Security Center (NOSC) manages the PACAF Time Compliance Network Order (TCNO) process IAW AFSSI 5021, *Time Compliance Network Order (TCNO) and Vulnerability and Incident Reporting. AFSSI 5021 will become AFMAN 33-225, Volumes 1 and 2.* The NOSC and Network Control Centers (NCCs) review audit, vulnerability, and security survey reports for applicability within the command. NCCs are responsible to implement measures to correct deficiencies.

2.9.1.7. HQ PACAF/SCP is the focal point to track and ensure MAJCOM compliance with C&A and C4ISP requirements for both unclassified (NIPRNET) and secret (SIPRNET) networks. HQ PACAF/SCI is responsible for the review of network security aspects of SSAA packages (i.e. communications ports, protocols, operating system software security features, passwords, administrative rights).

2.9.1.7.1. (Added) HQ PACAF/SCP will track status on all Interim Approval to Operate and Authority to Operate timeframes to ensure progress is being made by the Program Management Office (PMO) to complete the SSAA package as well as the C4ISP package.

2.9.1.7.2. (Added) HQ PACAF/SCP is responsible to monitor and track AFCA Certification of Networthiness (CoN) packages, PACAF Certificate To Operate (CTO) process, enforcing DITSCAP format standards with all PMOs fielding systems within PACAF. Additionally, PACAF/SCP is responsible for oversight and fielding of MAJCOM level systems within the PACAF Theater.

2.9.1.8. (Added) HQ PACAF/SCI will ensure the integration of Information Assurance activities and programs into the Command's Defensive Counter Information (DCI) program.

2.10.1.7. (Added) The Wing IA office will ensure the integration of wing Information Assurance activities and programs into the wing's DCI program.

2.10.1.8. (Added) COMPUSEC Account Records Management. Wing and unit COMPUSEC managers must maintain COMPUSEC account records in a 7-part folder or binder, or a 6-part folder or binder with a separate accreditation packages folder. At a minimum, the folder will contain the following sections:

2.10.1.8.1. (Added) Part 1 - Identification and training.

2.10.1.8.2. (Added) Letters appointing the wing/base/unit COMPUSEC manager and alternate.

2.10.1.8.3. (Added) A list of Unit COMPUSEC Managers (UCMs), and/or information system security officers (ISSOs) and/or terminal area security officers (TASOs) as applicable. Include training verification (this may include, but is not limited to: anti-virus software, internet use, consent to monitor, risk analysis, Certification and Accreditation, IA computer based training, passwords, helpful internet sites, policy letters, PACAF supplements, user training and DAA training).

2.10.1.8.4. (Added) Part 2 - Policy.

2.10.1.8.5. (Added) Security policies and accreditation information.

2.10.1.8.6. (Added) Site-specific network/system security guide (if not available, then system security guide/policy of oversight organization and/or system).

2.10.1.8.7. (Added) Spreadsheet of unclassified accredited systems (interim and full), unaccredited unclassified systems, spreadsheet of classified accredited systems (interim and full) and unaccredited classified systems.

2.10.1.8.8. (Added) Accreditation packages and supporting documentation (may be cross-referenced to another location).

2.10.1.8.9. (Added) ADPE listing of all systems within purview of local DAA representative (may be cross-referenced to another location) and any unit-unique IA procedures.

2.10.1.8.10. (Added) Part 3 - Metrics.

2.10.1.8.11. (Added) Time Compliance Network Order (TCNO)/CTO suspense compliance tracking spreadsheet (if maintained electronically, provide a cross-reference location).

2.10.1.8.12. (Added) Metrics documentation and correspondence.

2.10.1.8.13. (Added) Part 4 - EMSEC and Security Incident Correspondence.

2.10.1.8.14. (Added) Emissions Security (EMSEC) approval memorandum (for areas processing classified information. Completed AFCOMSEC Form 7001's are classified and therefore must be secured in an authorized container/location).

2.10.1.8.15. (Added) Security incident and virus reporting (includes virus incidents and detailed remanence security procedures and security violation reporting procedures).

2.10.1.8.16. (Added) Part 5 - IA Correspondence.

2.10.1.8.17. (Added) General correspondence, messages, and hand receipts for classified mailings.

2.10.1.8.18. (Added) Part 6 – Self Inspections.

2.10.1.8.19. (Added) A copy of the last Information Assurance Assessment and Assistance Program (IAAP) review and/or SAV IAW AFI 33-230 (Information Protection Assessment and Assistance Program). If the IA program has a COMSEC account, maintain as a minimum a copy of the COMPUSEC and EMSEC findings, as the complete report is already required to be maintained according to COMSEC account management. Include self-assessments and related information.

2.10.1.8.20. (Added) Wing COMPUSEC managers will maintain a folder for their overall wing COMPUSEC program, and a folder for each of their UCMs. UCMs will maintain their own folder with as near to identical information as the wing COMPUSEC manager. UCMs who also have classified systems within their area of responsibility will ensure they maintain EMSEC approval documentation provided by the supporting information assurance office's EMSEC manager.

2.10.2.1. (Added) NCCs will comply with guidelines directed in PACAF Special Instructions to Communicators (SINC). This document can be located at **https://nosc.pacaf.af.mil** home page.

2.11. Commanders appoint in writing a unit COMPUSEC manager to oversee their COMPUSEC program. An active duty or DoD civilian individual must fill the primary COMPUSEC position. Unless required by the MAJCOM or wing, official designation of ISSOs is at the discretion of the unit COMPUSEC manager. If the ISSO positions are not assigned, the ISSO responsibilities reside with the unit COMPUSEC manager.

3.2.1. COMPACAF exercises overall DAA responsibility for the command. HQ PACAF/SC is delegated PACAF MAJCOM DAA for unclassified (NIPRNET) and secret (SIPRNET) networks. This includes all PACAF-operated fixed and deployed networks within the PACAF Area of Responsibility (AOR). As the PACAF DAA, the PACAF/SC has overall approval authority for network configuration and architecture standards.

3.2.1.1. (Added) HQ PACAF/SC has the authority to direct wing DAAs to take specific actions in the best interest of the PACAF Enterprise Network for mission accomplishment by ensuring the availability and protection of our networks and business applications. These specific actions include (but are not limited to) directing network configuration changes and disconnection of local or wing networks that pose undue risk to the PACAF Enterprise Network or impact mission critical operations. The MAJCOM DAA will coordinate with affected commanders and the PACAF Information Operations Steering Group (IOSG) as necessary to determine operational impact prior to directing disconnection of any systems or networks. Sub-level IOSG organizations, including the PACAF Information Operations Working Group (IOWG), Information Operations Cell, PACAF Information Warfare Flights, and the PACAF Network Operations and Security Center, will assist IOSG efforts as tasked. Specific Information Operations roles and responsibilities are outlined in PACAF Instruction 10-705, *Information Operations*.

3.2.1.1.1. (Added.) The PACAF/SC (as MAJCOM DAA) is the single accreditation authority for all DoD, AF and PACAF command and control, business, common-user, and intelligence applications on all PACAF-operated fixed and deployed networks within the PACAF AOR (SIPRNET and NIPRNET). These include all Program Management Office (PMO)-managed, MAJCOM developed, government off the shelf (GOTS), and commercial off the shelf (COTS) applications. An application is defined as a program (software and program specific hardware such as servers) and may have both a client-side and a server-side, normally resides on the network, and typically targets a business process for a specific functional community or communities.

3.2.1.1.2. (Added) PACAF/SC certifies all applications on NIPRNET and SIPRNET through the Certificate to Operate process IAW PACAFI 33-102, *Introducing New Communications and Information (CI) Systems*. The Certificate to Operate is the single authorization and direction for wings to proceed with installation of the application on their networks. There is no further requirement for wings and or units to certify and accredit applications. Approved SSAA packages must be retained at the base as part of the overall security package. Site requirements not specifically listed in the overall SSAA package will be accomplished by the responsible office at each installation. Once certified, the PACAF NOSC will coordinate application installation with the base NCCs through the PACAF Communications Task Order. If a wing NCC identifies a security risk or other problem concerning an application during fielding that was not identified in the Certificate to Operate package, local DAAs will immediately notify the MAJCOM DAA Representative (HQ PACAF/SCP action officer) via SIPRNET and courtesy copy PACAF/SCI and the PACAF NOSC. The Wing IA office will provide PACAF/SCP action officer with a brief synopsis of the issues and security concerns. PACAF/SCP action officers will take appropriate action to validate security concerns with PACAF/SCI. PACAF/SCP will make a recommendation to the PACAF/SC to proceed with fielding or suspend the Certificate to Operate.

3.2.1.1.3. (Added) The PACAF/SC deputy director may serve as MAJCOM DAA in the absence of the director. Further delegation is not authorized.

3.2.1.1.4. (Added) The Defense Intelligence Agency (DIA) is the DAA for the DODIIS community and the National Security Agency (NSA) is the DAA for NSANET. DIA and NSA hold sole DAA delegation authority for those communities. The 690 ISS/PIA serves as the DAA representative and Air Force Service Certifying Organization for SCI systems and applications. HQ PACAF/INS is the MAJCOM Information Systems Security Manager (ISSM). HQ PACAF/INS and the site DODIIS ISSMs are the certification and accreditation authority for stand-alone SCI applications and systems operating inside a DODIIS SCIF IAW Joint DoDIIS/Cryptologic SCI Information Systems Security Standards and Director of Central Intelligence Directive (DCID) 6/3, Protecting Sensitive Compartmented Information Within Information System.

3.2.1.2. Wing Commanders are delegated wing network DAA responsibilities for their portion of the network infrastructure, including all workstations, printers, networked copiers, all standalone systems, scanners and any other networked devices owned by tenant units, headquarters units, HQ PACAF, Numbered Air Forces (NAF), and subordinate Geographically Separated Units (GSU).

3.2.1.3. (Added) Wing network DAAs will certify their networks meet DoD, Air Force and HQ PACAF/SC security and configuration management requirements. Wing DAAs must ensure units install applications in compliance with the PACAF network type accreditations and Certificate to Operate if such applications interface with other PACAF bases through Firewall/Router ports. If an application is site specific then Wing Network DAAs may approve locally.

3.2.1.4. (Added) Wing Vice Commanders may serve as wing network DAA when acting in the capacity of the Wing Commander. Further delegation is not authorized.

3.2.1.5. (Added) HQ PACAF/SC serves as interim DAA for PACAF-sponsored deployed networks until an operational or site commander takes command of the site.

3.5. This section applies to all information systems used by only one individual at a time. The PC or workstation may be operated as a stand-alone system or connected in a network environment. (NOTE: Information systems that allow file sharing over a network must comply with the requirements of multi-user information systems [paragraph 3.6].) Stand-alone systems represent the simplest in terms of protection requirements and certification level-of-effort. These systems have no network connectivity or modem/fax capability at any time and operate in a dedicated or system high security mode of operation. All that is required to certify and accredit these systems is to complete a worksheet similar to the sample provided at **Attachment 7 (Added)**.

3.5.1.1. Verify each user's need for access to information systems resources and information. Follow identification and authentication procedures according to AFMAN 33-223, *Identification and Authentication*. Summer hires, temporary hires and volunteers for employment to last 180 days or less may be granted access without the National Agency Check (NAC) or equivalent IAW AFSSI 5027 para 5.3.1, *Network Security Policy* and AFI 31-501, *Personnel Security Program Management* requirement providing the following conditions are met:

3.5.1.1.1. (Added) Unit security managers initiate local files check (LFC).

3.5.1.1.2. (Added) Security Forces verify to unit commander the LFC has been conducted.

3.5.1.1.3. (Added) Unit commander grants access based on suitability determination.

3.5.1.1.4. (Added) User completes network user training requirements identified in AFI 33-115 Volume 2, *Licensing Network Users and Certifying Network Professionals*.

3.5.1.1.5. (Added) The supervisor and system administrator/workgroup manager have implemented appropriate security controls.

3.5.3.1.1. (Added) Reference PACAF PDA policy letter for further guidance at **https://www.hqpacaf.af.mil/sc/scn/SCNI/cip/default.html**

3.7.3. Request to grant foreign national access to information systems refers to PACAF owned and controlled, unclassified sensitive information network or information system (IS), and the information contained therein. This means access by foreign national individuals to PCs, workstations or other computer systems on a PACAF owned and controlled unclassified LAN in the pursuit of US interests. The term foreign national includes persons that are either a Direct or Indirectly hired foreign national civilian employed full-time or part-time in a position on base using a PC in the commander's outer office, a foreign national civilian in a position requiring access to a PC to fulfill short-term requirements while supporting US interests, to include humanitarian relief missions, or a foreign national military member in a Liaison or Exchange position, foreign military members participating in US-hosted exercises, or other individuals approved by PACAF/CV.

3.7.3.1. The basic requirement for access is the same in each case: US Interests must be clearly shown, the IS must be owned and controlled by a PACAF organization, foreign disclosure must be taken into consideration, user training is completed IAW AFI 33-115 Volume 2, *Licensing Network Users And Certifying Network Professionals,* and NAC or equivalent requirements have been favorably satisfied. This

section does not refer to access by foreign national organizations (i.e. giving access based purely on membership of any particular organization), access to NIPRNET or the Defense Information System Network (DISN) backbone, or connection of foreign-owned equipment to any part of the network. The PACAF/CV is the lowest level approval authority to allow foreign nationals access to a network or IS, owned and controlled by PACAF, running business applications and common-user applications such as e-mail, web access, and local shared file directories. While the requirements for access are not new, in PACAF it is the positions or billets themselves that are approved or disapproved, and the unit commander must then ensure that IAW CJCSM 6510.01, AFI 31-501, and DOD Publication 5200.2-R the foreign national requiring access meets the requirements of that position or billet as listed in Table A11.1 at **Attachment 11(Added)**, or access must be denied until requirements are met. Foreign nationals cannot be granted interim or limited access. This procedure both aids the administration of the approval process and aids the hiring process since position requirements are now much clearer.

3.7.3.2. IG teams will inspect unit compliance.

3.7.3.3. Foreign nationals may only access computers that run the Microsoft Windows NT® or higher operating system, or any similar operating system that incorporates PACAF required access controls. Use access controls to restrict foreign national access to Foreign Disclosure Office (HQ PACAF/FDO) approved information. Foreign national investigative requirements for access to unclassified e-mail, file, and print services are identified in AFI 31-501.

3.7.3.4. Approval Process. The HQ PACAF/CV will review updates for approval/disapproval on a monthly basis. This approval is valid only for as long as the position or billet exists, and the requirement is valid, up to 2 years. After 2 years, units must reapply for HQ PACAF/CV approval.

3.7.3.5. Unit. Before authorizing foreign national access the unit will:

3.7.3.5.1. (Added) Identify the need for foreign national access, and then identify the foreign nationals by position or billet. The unit then builds a Request for Access package for HQ PACAF/CV approval. A unit Request for Access package consists of:

3.7.3.5.1.1. (Added) Cover letter from the unit commander to the Wing Commander (see **Attachment 8 (Added)**). This letter should include the following information:

3.7.3.5.1.2. (Added) Brief mission statement and current environment description.

3.7.3.5.1.3. (Added) Organizations involved and a point of contact.

3.7.3.5.1.4. (Added) List of individuals performing FSA or WM duties on the PCs and LAN (foreign national or US).

3.7.3.5.1.5. (Added) Statement certifying that access is required for the performance of assigned duties and is in US interests.

3.7.3.5.1.6. (Added) Statement certifying that the foreign national will not have access until he or she has had a NAC or equivalent, user training IAW AFI 33-115 Volume 2, *Licensing Network Users And Certifying Network Professionals*, and HQ PACAF/CV approval.

3.7.3.5.1.6.1. (Added) For foreign participants at US-hosted exercises, the visiting nation must submit a request for those deployed members requiring base network and system access through the US Embassy in their country at least 2 months before the exercise. This will initiate a foreign disclosure review that will flow down from SAF/IA to PACAF/IN (foreign disclosure). The wing (host base) commander(s) for the exercise will provide a statement certifying that the foreign national will not have access until he or

she has been approved by this process, had user training IAW AFI 33-115 Volume 2, and HQ PACAF/CV approval.

3.7.3.5.2. (Added) Foreign disclosure release statement.

3.7.3.5.3. (Added) Spreadsheet showing details of the foreign national positions or billets. Spreadsheets will contain the following fields/information:

3.7.3.5.3.1. (Added) Position identifier or billet number.

3.7.3.5.3.2. (Added) Organization/office symbol.

3.7.3.5.3.3. (Added) Position title.

3.7.3.5.3.4. (Added) Duties requiring access (i.e., "process real-estate data and provide to the wing civil engineer").

3.7.3.5.3.5. (Added) Nationality.

3.7.3.5.3.6. (Added) Specific business and common user applications and data description (i.e. "MS Office 97, ABSS, email, and Air Tasking Orders", or "Privacy Act Data, Global Decision Support System (GDSS), Air Mobility Tracking and Scheduling Data"). If access to financial data is required, state if it exceeds $10 million.

3.7.3.5.3.7. (Added) Frequency required (i.e. "Normal Office Use", "Constant stream of FTP data", or "occasional e-mail use, once per week average").

3.7.3.5.3.8. (Added) Restriction Methods. List the access controls employed to restrict foreign national access to information the foreign national needs to perform duties, and which the foreign disclosure office approved for release to the foreign national's nation. At a minimum, set up user permissions to permit access only to specific directories and files. Data accessed via web browsers has it's own control IAW AFI 33-129, Table 1, and PACAF Supplement 1 to AFI 33-129, Table 1, so controlling access by foreign nationals to specific websites would be redundant and unrealistic.

3.7.4. Once approved, grant network access to approved individuals and limit access to the extent necessary to perform assigned duties. No other specific "system" access (i.e. MILMOD, NTFS, VSAT) can be granted. System-Level DAA's are responsible for granting individual access to their respective DOD/AF/Joint system(s) residing on NIPRNET, even though "network" access has already been granted. The system DAA grants access to the information systems and Designated release/disclosure authority grants access to information.

3.7.5. Routing and unit responsibilities. This section outlines the steps each unit takes to obtain foreign national access approval. See **Attachment 12(Added)** for Foreign National Access approval process flow chart.

3.7.5.1. Unit. The unit identifies positions requiring access and required information. The unit completes Request for Access Packages and forwards these packages to HQ PACAF/FDO for foreign disclosure review. The Foreign Disclosure Office reviews the package, works with the unit to resolve disclosure issues, attaches a foreign disclosure release statement to the package if it meets requirements, and returns the package to the unit. Blanket statements can be used in cases of large numbers with the same requirements and circumstances. The unit receives the package and forwards it to their wing IA office.

3.7.5.2. Wing IA Office. The wing IA office logs and tracks unit packages. The wing IA office consolidates these packages and forwards consolidated packages to the wing commander for review and signature. See **Attachment 9 (Added)** for a sample foreign national access letter.

3.7.5.3. The wing commander reviews and approves packages, then forwards to HQ PACAF/SC.

3.7.5.4. The PACAF/SC reviews the submitted package and forwards to HQ PACAF/DS.

3.7.5.5. (Added) HQ PACAF/DS. HQ PACAF/DS collects wing packages for HQ PACAF/CV endorsement on a monthly basis. Urgent packages such as for humanitarian relief or other short-notice operations are accomplished as soon as can be processed.

3.7.5.6. (Added) HQ PACAF/CV. HQ PACAF/CV indorses access request letters and HQ PACAF/DS returns the packages to the wing IA offices. HQ PACAF/DS provides a copy of access letter back to the PACAF/SC.

3.7.5.7. (Added) Wing IA Office. The wing IA office keeps the wing packages on-file, and sends a memorandum to the unit notifying them of approval of foreign national access for their positions or billets. They work with the unit to update C&A packages and obtain DAA approval. They help the unit where they can to address any disapproved packages. The wing IA office forwards the NCC a copy of the spreadsheet showing which position identifiers or billet numbers have been approved and copy of CV memo. Records required by this paragraph will be maintained under AFMAN 37-139, Table 31-8, Rule 6.

3.7.5.8. (Added) NCC. The NCC maintains accounts for foreign nationals only when the individual is matched against an approved foreign national position identifier or billet number. They will maintain a modified spreadsheet to track (i.e. add individual's names next to each approved position identifier or billet number on the spreadsheet provided by the wing IA office). The NCC creates new accounts and modifies existing accounts to include "FN" and country after the name and rank (i.e. Bond James Commander FN JP 18CS/WWW). The NCC deletes the account upon notification from the unit or expiration of CV memo and updates the spreadsheet accordingly.

3.7.5.9. (Added) Unit. The Wing IA notifies the NCC when accounts need creating or deleting, giving the associated position identifier or billet number along with the individual's details. The unit commander has responsibility for ensuring that individuals in these positions or billets meet the requirements listed in Table A11.1 at **Attachment 11(Added)**. The unit must work with the wing IA office to identify foreign national access in C&A packages. The unit will ensure all foreign nationals in an approved billet/position have NAC or equivalent checks and user training before requesting accounts. The unit identifies new foreign national information requirements and forwards these requirements to HQ PACAF/FDO for review and inclusion in an updated foreign disclosure statement. The unit resolves disclosure issues with PACAF/FDO and forwards disclosure packages to the wing IA office. The unit will maintain all records related to foreign national access requests, foreign disclosure and account requests in accordance with AFMAN 37-139, Table 31-8, Rule 6.

3.7.5.10. (Added) For COMPACAF-directed access, HQ PACAF/SC will complete the Request for Access package for the required positions and billets, coordinate as needed, and forward to HQ PACAF/CV for review. HQ PACAF/CV will forward a memorandum to the host wing commander informing him or her of approval and provide a courtesy copy to the PACAF/SC (**Attachment 10 (Added)**).

3.7.5.11. (Added) Access approval for visiting foreign nationals. Visiting foreign nationals may require access to PACAF owned and operated automated information systems in the course of their PACAF visit. An example of this situation occurs when foreign nationals deploy to a PACAF installation in support of

an exercise such as COPE THUNDER. PACAF/CV must approve foreign national access requirements for each separately scheduled exercise. The process to authorize access to the PACAF enterprise network varies greatly, depending on the type of access required, what systems the foreign nationals need access to, and what access to US networks they may already have (sponsored by another command).

3.7.5.11.1. (Added) Basic requirements that must be met to authorize visiting foreign national access to the PACAF enterprise network is the same as requirements for other foreign national categories: US Interests must be clearly shown, the IS must be owned and controlled by a PACAF organization, foreign disclosure must be taken into consideration, user training is completed IAW AFI 33-115 Volume 2, *Licensing Network Users And Certifying Network Professionals,* and NAC or equivalent check requirements have been favorably satisfied.

3.7.5.11.2. (Added) The US sponsor for the foreign national visit will submit a foreign national access request to PACAF/SCI early in the planning stages of the visit.

3.7.5.11.3. (Added) PACAF/SCI will review the request and determine what actions are required to grant access to the PACAF network enterprise. If PACAF/CV is required, PACAF/SCI will assist the US sponsor with completion of the Request for Access package.

3.8.1.1. (Added) System administrators/workgroup managers will apply PACAF NOSC provided lock-down procedures on automated information systems utilizing a Microsoft Operating System prior to placing them on the PACAF Enterprise network. NOSC developed lock-down procedures are developed to mitigate known "out of the box" vulnerabilities associated with various Microsoft operating systems and are available for download from the NOSC web site: **https://nosc.pacaf.af.mil/** .

3.8.1.2. (Added) Internet Security SafeSuite Internet Scanner (ISS) is the Air Force's network scanning tool of choice and is fielded at all PACAF bases as part of the Combat Information Transport System/Network Management System /Base Information Protect (CITS NMS/BIP) initiative. ISS provides some system configuration validation to mitigate known system vulnerabilities. All PACAF bases will perform quarterly network vulnerability scans using ISS and the NOSC provided custom scanning policy. In addition, new automated information systems must be scanned using ISS before they are permanently installed onto the base's network infrastructure. ISS scans are not required for standalone systems.

3.8.1.3. (Added) PACAF Vulnerability and Assessment program (VA Tracker) is required to be installed on all NCC ISS workstations. This program further contributes to the integrity of the completed ISS scans by enabling the NCC to assign Internet Protocol (IP) ranges to specific WMs throughout their area of responsibility. NCCs will have the capability to filter out "false positives" and all "acceptable" risks giving a clearer picture of overall network security. This program enables NCCs and WMs to track overall progress (via e-mail) by all WMs. This program is not required to be loaded on any other system on the base network.

3.10.4.3. (Added) Personal PDA use is authorized as specified in paragraph 3.5.3.11. Downloading of games to the PDA is strictly forbidden.

3.11.1. Restrict information system maintenance to authorized personnel with a security clearance for the highest classification and most restricted category of information processed. Qualified foreign nationals who are properly cleared to access unclassified networks and business applications IAW section 3.7 and related attachments of this supplement may perform maintenance activities on unclassified systems only. Maintenance on any IS, to include PCs, servers, digital copiers or printers, or any other equipment with disk drives, memory, or network capabilities, used for processing classified material, even once, must be performed using the following procedures:

3.11.1.1. (Added) Maintainers will be US citizens with a clearance at the same level as the equipment being worked on. If the installation cannot obtain a maintainer with an appropriate clearance, or the only maintainer available is a foreign national, then he/she must be escorted by an individual with an appropriate clearance and the ability to identify unauthorized activity. This can be a workgroup manager or functional system administrator. The escort will verify the maintainer's identity. Uncleared individuals may perform maintenance on information systems used to process classified information only if the information is sanitized.

3.11.1.2. (Added) Disconnect networked equipment prior to maintenance. If the equipment is a copier, fax, or printer, check for and clear paper jams.

3.11.1.3. (Added) If the maintainer uses a laptop or other device with the ability to retain data for maintenance or diagnostics, the laptop becomes classified to the same level of classification of the system being repaired. Therefore, only maintainers with appropriate clearances may remove the maintenance laptop from the unit. If an uncleared maintainer uses a laptop for maintenance, the laptop must be US government-owned and must remain with the unit when the maintainer departs to prevent inadvertent disclosure. The escort must observe the screen of any such laptop to verify no sensitive or classified information is disclosed. If an uncleared maintainer uses diskettes to perform maintenance, the disks must remain with the unit. If the laptop used is not one labeled for the classification used, then the disk drive must be removed and labeled accordingly. Proprietary software can be removed from the laptop when maintenance is finished.

3.11.1.4. (Added) Any memory modules, disk drives, or any other component with the ability to retain data that is removed from the equipment must remain with the unit and be disposed of according to the highest classification of data used on the equipment or be sanitized IAW AFSSI 5020, *Remanence Security*.

3.11.2.1. (Added) Remote maintenance or administration on a PACAF information system that uses an encrypted TELNET session is authorized, but must be documented in the C&A package.

3.11.2.2. (Added) All systems will be removed from the TELNET port access control lists on all PACAF base firewalls. If a system administrator requires access to a system via clear text TELNET, they must coordinate with the appropriate base network control center to have the port opened for a specified period of time, normally not to exceed one hour. NCCs will establish and coordinate local procedures with system administrators requiring clear text TELNET access in advance to ensure access can be expeditiously obtained to minimize system downtime.

3.11.2.3. (Added) If foreign nationals perform remote maintenance or administration, follow foreign national access procedures IAW paragraph 3.7.

3.18. (Added) Passwords. Applying password protection is one layer of defense that is not costly, yet is often the weakest link in our network security posture.

3.18.1. (Added) All passwords will be generated, utilized, maintained, and protected IAW AFM 33-223, *Identification and Authentication* at a minimum.

3.18.2. (Added) The applicable system's certification and accreditation (C&A) will clearly identify password generation, usage, maintenance and protection, and will comply with all applicable security directives. Requirements may be more restrictive than current guidance, but will never be less restrictive when technically feasible.

3.18.3. (Added) All users will be instructed on the password policies and requirements for the applicable systems that they are granted access to.

3.18.4. (Added) Passwords associated with administrative accounts require special emphasis.

3.18.4.1. (Added) Apply more stringent password construction requirements where deemed appropriate. In most cases, administrator passwords should have a minimum of 12 alphanumeric characters, where 2 are numeric and 1 is a special character.

3.18.4.2. (Added) Consider implementing a shorter password aging policy than currently applied to user level accounts.

3.18.4.3. (Added) Enable auditing on administrative accounts.

3.18.4.4. (Added) Limit the number of administrative accounts assigned and stress administrative account logins should be used to perform administrative functions only.

3.18.5. (Added) Should a conflict arise between applicable security directives, the more restrictive of them will be imposed.

3.18.6. (Added) Password Policy Enforcer (PPE) must be installed on all Windows NT/2000 Primary and Backup Domain Controllers. Installation on Windows based clients is optional. PPE is available for down load at **https://nosc.pacaf.af.mil/nosc/security/ppe/index.html**.

3.18.7. (Added) All PACAF NCCs will run a password crack program and report the results to the PACAF NOSC IAW NOSC Directives.

4.2.1.1.1. (Added) Wing and functional program managers shall ensure all PACAF personnel, who are responsible for certification and accreditation, are provided training on DoD and PACAF C & A process, AF C4ISP process, PACAF CTO process, policies, and regulations.

4.2.1.1.2. (Added) Refer to PACAF Supplement to AFI 33-102 for direction on timeframes for the completion of SSAA packages. Additionally, this supplement outlines consequences for not meeting established timeframes.

4.2.1.1.3. (Added) HQ PACAF/SCP will develop and maintain a method for identifying and tracking the C&A status of software, systems, and networks operating in PACAF.

4.2.1.1.4. (Added) The communications squadron or communications group commander serves as the Wing DAA representative.

Attachment 1

References

DoD 5200.2-R, Department of Defense Personnel Security Program

AFI 31-501, Personnel Security Program Management

AFI 33-129, Transmission of Information via the INTERNET

AFMAN 37-139, Records Disposition Schedule

PACAF Instruction 10-705, *Information Operations*

PACAF Instruction 33-102, Introducing New Communications and Information (CI) Systems

PACAF Supplement 1 to AFI 33-129, Transmission of Information via the INTERNET

Abbreviations and Acronyms

(Added) IS—Information System

Terms

Business Applications——A system (software and program-specific hardware such as servers) that has both a client-side and a server-side, and typically targets a business process for a special functional community or communities.

Networks——The physical infrastructure used to access and transmit data between business applications via a computer.

Attachment 7 (Added)

SAMPLE STAND-ALONE INFORMATION SYSTEM CERTIFICATION/ ACCREDITATION WORKSHEET

Stand-alone systems represent the simplest in terms of protection requirements and certification level-of-effort. These systems have no network connectivity or modem/fax capability at any time and operate in a dedicated or system high security mode of operation. Completion of the attached will satisfy all MAJCOM specified stand-alone certification and accreditation requirements. Additional requirements may be required based on local guidance. Consult the wing IA office for specific guidance.

PACAF STAND-ALONE INFORMATION SYSTEM CERTIFICATION/ACCREDITATION WORKSHEET

System Description

1. Identify the ISSO: Rank/Grade: _____ Name: _____

2. Classification(s) of System (check all that apply): Sensitive _____ Secret _____ Top Secret _____

3. Categories (check all that apply): PA _____ FOUO _____ PROPIN _____ Name Other(s): _____

4. Identify System: Processor Type (i.e., Pentium, Celeron, AMD): _____

5. Serial Number(s): _____

_____

7. List of Peripherals: _____

8. System/Information Criticality (Choose One): Non- mission Essential _____ Mission Impaired _____ Mission Essential _____ Mission Critical _____

9. Usage (Choose one): Single-User _____ Multiple User _____

10. Review Date/Initials: _____ _____ _____ _____ _____ _____ _____ _____ _____

System Security Policy

The system operates only as a stand-alone in either system high or dedicated security mode of operation. It is not networked nor does it have connectivity to a modem/fax (internal or external). Wing Network DAA accreditation is obtained prior to system operation. Any change to system configuration, mode of operation, classification, location, operating system, procedures, etc., triggers recertification/ reaccredidation actions. Additionally, all software add-ons (i.e., applications) are certified prior to installation and do not invalidate this security policy.

Access to sensitive/classified information is limited to authorized personnel cleared to the highest level and most restrictive category. When unauthorized personnel are in the area, protection is provided for printer output and monitor screens to assure sensitive/classified information cannot be casually viewed. Approved procedures are used to purge, clear, or destroy media used to store sensitive/classified information before release to unauthorized personnel.

The system and information are safeguarded against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, or release to unauthorized persons. Hardware, firmware, software, documentation, and information are protected at the highest level of classification/sensitivity jeopardized to prevent unauthorized disclosure, destruction, or modification. Protection of the system is provided to the hardware and software against theft according to AFI 31-209, *The Air Force Resource Protection Program*. Continuity of operations is assured for critical functions.

The appropriate level of emission security (EMSEC) protection is provided when the information system and peripheral devices are used to process classified information or to coexist with information systems that process classified information (AFI 33-203).

The operational system is protected, at a minimum, as sensitive and provides C2 criteria class functionality as outlined in DoD 5200.28-STD and AFSSI-5027 and AFMAN 33-223 which includes unique user identification and authentication, audit, discretionary access control, and object reuse. Where possible, the system uses computer-based security. Additionally, PACAF NOSC operating system lockdown procedures will be applied. Output products, removable media, and printer ribbons are safeguarded, marked, and labeled as required by AFI 31-401 until destroyed or declassified using procedures in AFSSI 5020. The information system clears and overwrites memory and storage space prior to release back to the operating system for reallocation to the system (AFSSI 5020). When changing from one classification level to a lower level, the user(s) purges the information system's memory before processing at the new level. Storage media that is nonvolatile and writeable (e.g., magnetic media such as hard disk and floppy disks/diskettes) is/are protected for the highest classification processed on the information system. The system meets one of the conditions listed below when using nonvolatile, nonremovable storage media to process classified information:

· The information system is installed in an area approved for open storage of classified information by the installation commander at or above the highest classification level of the information processed.

· The information system uses a Wing Network DAA-approved product or technique to prevent storage of classified information on nonvolatile, nonremovable storage media, and the information system is certified and accredited to operate as such.

· The information system is protected and stored according to AFI 31-401.

PACAF STAND-ALONE INFORMATION SYSTEM CERTIFICATION/ACCREDITATION WORKSHEET

ST&E Checklist	Yes	No	N/A
1. Is the ISSO familiar with his/her duties? (AFI 33-202)			
2. Does the ISSO have an adequate technical background (e.g., computers and security) to perform this certification and perform his/her duties? (AFI 33-202)			
3. Does the ISSO maintain the system's C&A documentation (i.e., this checklist)? (DoD 8510.1-M)			
4. Has the ISSO established and managed a COMPUSEC training program for system users? (AFI 33-202)			
5. Has the ISSO developed and implemented procedures for handling of security incidents? (AFSSI 5021)			
6. Is the system usage audited? (AFSSI 5027)			
7. Does the system comply with the system security policy (on front of worksheet)? (AFI 33-202)			
8. Are default vendor accounts, privileges, and passwords deleted? (AFSSI 5027, PACAF NOSC NT/2000 Lockdown Procedures)			
9. Is authentication (e.g., user-id and passwords) unique to each user? (AFSSI 5027, AFMAN 33-223)			
10. Is each user's authentication changed quarterly? (AFSSI 5027, AFMAN 33-223)			
11. Are group accounts disallowed or in compliance with AFMAN 33-223 directives?			
12. If passwords are used, are they at least 8 characters in length? (AFMAN 33-223)			
13. Are procedures in place to ensure that dictionary-type words are not used as passwords? (AFMAN 33-223)			
14. Are controls in place to ensure timely removal of user accounts when no longer needed? (AFI 33-202)			
15. Are users only given the minimum capabilities/privileges required to perform their assigned duties? (PACAF NOSC NT/2000 Lockdown Procedures, AFSSI 5027)			
16. Do all personnel gaining access to the system have a validated need-to-know? (AFI 33-202, AFI 31-501)			
17. Do all users have a valid clearance for the highest classification level and authorization for all categories of information for which they could have access to? (AFI 33-202, and AFI 31-501)			
18. Are procedures in place to protect against inadvertent access to sensitive/classified information by uncleared personnel (e.g., visitors, maintenance personnel, etc.)? (AFI 33-202, AFI 31-501)			
19. Have procedures been established for purging/clearing sensitive/classified information from the system? (AFSSI 5020)			
20. Is current anti-virus software installed and properly used on the system? (AFSSI 5027, PACAF NOSC NT/2000 Lockdown Procedures).			
21. Are users aware of proper reporting procedures for security incidents, vulnerabilities, and virus attacks? (AFSSI 5102, 5021)			
22. Have appropriate contingency/emergency plans been developed and tested to ensure continued availability and integrity of the system and data? (AFI 33-202, AFMAN 10-401)			
23. Are system backups made routinely for mission critical and mission essential data? (AFSSI 5027)			
24. Are required security countermeasures (i.e., patches, etc.) implemented to correct known vulnerabilities? (AFI 33-202, AFCERT Time Compliance Network Orders (TCNO)).			
25. Have procedures been established for the proper disposal/destruction of system products (e.g., listings, disks, tapes)? (AFSSI 5020 and AFI 31-401)			
26. Are all products produced by the system (e.g., listings, tapes, disks) marked with the highest classification/category of the system? (DoDD 5200.1 and AFI 31-401)			
27. Has the wing IP office accomplished an EMSEC assessment for the system? (AFI 33-203)			
28. Are information system hardware and software protected against theft? (AFSSI 5027, AFI 33-202, AFI 31-209)			
29. Are systems and information protected against tampering? (AFSSI 5027 and AFI 33-202)			
30. Has a notice to consent to monitoring notice been applied as a log in banner? (AFI 33-219 Attachment 2 section C)			

Certifying Official's Validation	Wing Network DAA's Accreditation Approval
Date Submitted: _____	**Date Approved:** _____
Signature: _____	**Signature:** _____
Name: _____	**Name:** _____
Title: _____	**Title:** _____
Accreditation Control Number: _____	**Accreditation Expiration Date:** _____

Page 2 of 2

Note: This worksheet constitutes the entire SSAA for Stand-Alone Information Systems.

Attachment 8 (Added)

SAMPLE FOREIGN NATIONAL ACCESS LETTER, UNIT/CC TO WING/CC

MEMORANDUM FOR (WING COMMANDER)

FROM:	(UNIT COMMANDER)
SUBJECT:	Foreign National Access to Unclassified Sensitive Information Automated Information Systems.

1. This letter is to notify you of our foreign national positions (at attachment) requiring access to unclassified sensitive information automated information systems. I certify that IAW PACAF Supplement 1 to AFI 33-202:

a. Access by the foreign national positions listed is required for the performance of assigned duties and is directly beneficial to the US government.

b. Access will be restricted to information certified releasable by PACAF/FDO.

c. Access will not occur until applicable certification and accreditation packages are updated and signed to reflect access by these foreign national positions.

d. Access will not occur until personnel filling these positions have successfully completed user training IAW AFI 33-115 Volume 2, *Licensing Network Users And Certifying Network Professionals*.

e. Access will not occur until personnel filling these positions have had a favorable National Agency Check (or equivalent) completed.

f. Access will not occur until authorized by PACAF/CV.

g. (Military/foreign national/contractor) personnel assigned to (unit) will perform Functional System Administrator (FSA) and/or Workgroup Manager (WM) duties.

2. Our mission is to provide the best real estate services possible to all units on this base. The working environment for the foreign nationals listed includes use of PCs operating Windows NT, attached to the unclassified base LAN, and running the Real Estate Planning, Tracking And Management Program (REPTAMP) utilizing FOUO unclassified data. Any financial information does not include amounts exceeding $10 million.

3. My point of contact for this issue is _____, DSN xxx-xxxx.

Unit Commander's Signature Block

Attachments:

1. Foreign national positions or billets spreadsheet (IAW PACAF Supplement 1 to AFI 33-202).
2. Memorandum from Foreign Disclosure Office authorizing release of specified information.
3. Memorandum from Security Forces and Attachment six.
4. Memorandum from Workgroup Manager verifying user training completed (IAW AFI 33-115 V2)

Attachment 9 (Added)

SAMPLE FOREIGN NATIONAL ACCESS LETTER, WING/CC TO PACAF/CV

MEMORANDUM FOR PACAF/CV

FROM:	(WING CC)
SUBJECT:	Request Approval of Foreign National Access to Unclassified Sensitive Information Automated Information Systems.

1. This letter is to request approval IAW PACAF Supplement 1 to AFI 33-202 for access to PACAF owned and controlled unclassified sensitive information automated information systems by foreign national positions or billets (at attachment). I certify that:

a. Access by the foreign national positions listed is required for the performance of assigned duties and is directly beneficial to the US government.

b. Access will be restricted to information certified releasable by PACAF/FDO.

c. Access will not occur until applicable certification and accreditation packages are updated and signed to reflect access by these foreign national positions.

d. Access will not occur until personnel filling these positions have successfully completed user training IAW AFI 33-115 Volume 2, *Licensing Network Users And Certifying Network Professionals*.

e. Access will not occur until personnel filling these positions have had a favorable National Agency Check (or equivalent) completed.

f. Access will not occur until authorized.

2. Mission and working environment for the foreign nationals listed has been provided to me by each unit, and includes use of PCs operating Windows NT or 2000, attached to the unclassified base LAN, in some cases running specific applications utilizing FOUO unclassified data as required by job duties.

3. My point of contact for this issue is _____, DSN xxx-xxxx.

Wing Commander's Signature Block

Attachments:

1. Foreign national positions or billets spreadsheet (IAW PACAF Supplement 1 to AFI 33-202).
2. Copy of current Certification and Accreditation letter.
3. Memorandums from Foreign Disclosure Office to units in the wing authorizing release of specified information.

1st Ind, PACAF/CV Date

MEMORANDUM FOR (WING CC)
I approve / do not approve access by the foreign national positions listed at the attachment.

PACAF/CV Signature Block

Attachment 10 (Added)

SAMPLE FOREIGN NATIONAL ACCESS APPROVAL MEMO

MEMORANDUM FOR (Wing Commander)

FROM:	PACAF/CV
SUBJECT:	Foreign National Access to Unclassified Sensitive Information Automated Information Systems

1. IAW PACAF Supplement 1 to AFI 33-202 for access to PACAF owned and controlled unclassified sensitive information automated information systems by foreign national positions or billets, I authorize access for the positions or billets listed at attachment 1 under the provisions that:

a. Access by the foreign national positions listed is required for the performance of assigned duties and is directly beneficial to the US government.

b. Access will be restricted to information certified releasable by PACAF/FDO.

c. Access will not occur until applicable certification and accreditation packages are updated and signed to reflect access by these foreign national positions.

d. Access will not occur until personnel filling these positions have successfully completed user training AFI 33-115 Volume 2, *Licensing Network Users And Certifying Network Professionals*.

e. Access will not occur until personnel filling these positions have had a favorable National Agency Check (or equivalent) completed.

2. Mission and working environment for the foreign nationals listed has been provided to me by each unit, and includes use of PCs operating Windows NT or 2000, attached to the unclassified base LAN, in some cases running specific applications utilizing FOUO unclassified data as required by job duties.

PACAF/CV Signature Block

Attachments:

1. Foreign national positions or billets spreadsheet (IAW PACAF Supplement 1 to AFI 33-202).

2. Memorandum from Foreign Disclosure Office (PACAF/FDO) authorizing release of specified information.

Attachment 11(Added)

REQUIREMENTS FOR ACCESS TO UNCLASSIFIED SENSITIVE INFORMATION PACAF AUTOMATED INFORMATION SYSTEMS

Table A8.1. Requirements for Access to Unclassified Sensitive Information PACAF Automated Information Systems (PCs, E-Mail Accounts, Web Browser, Etc) with Remarks.

Foreign National Status	Requirements
A. Foreign National (FN) civilian employed directly or indirectly by the US Government in accordance with Status of Forces Agreement (SOFA)	1. Determine the exact information, business and common-user applications required by the FN personnel (e-mail, specific web-sites, specific shared folders, specific software/data, etc). Unit commander must certify that access to the information is required for job performance and is directly beneficial to the US government. 2. Determine nationality of FN personnel requiring access. 3. Determination by the PACAF Foreign Disclosure Office of what information is releasable to the FN personnel for particular nationality and position or billet. Access is not allowed to any unclassified information system containing information that is controlled under the Arms Export Control Act, the Privacy Act, and exemptions to the Freedom of Information Act unless it is approved by the system DAA and the local Foreign Disclosure Officer. 4. All personnel, including FNs, must complete user training prior to access to any unclassified IS. 5. All personnel, including FNs, must have a National Agency Check or equivalent performed prior to access to any unclassified IS IAW AFSSI 5027 and AFI 31-501. Foreign nationals employed directly or indirectly by the US Government, to include contractors, require host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and a Defense Clearance and Investigations Index (DCII) Check; and an FBI-HQ/ID where information exists regarding residence by the foreign national in the United States for one year or more since age 18. Foreign military members require an equivalent NAC or equivalent conducted by their government. 6. Determine who will perform WM and SA duties on the hardware. 7. PACAF/CV is the lowest authority able to approve access by foreign nationals to any PACAF controlled unclassified sensitive information IS. In addition to the above, the request package must include: - A brief mission statement and description of current environment. - Organizations involved and POCs. - Specific information and applications required (E-mail, specific business application, specific web sites and/or pages, etc). - What and how often information will be transmitted.

	- Determination by the MAJCOM Foreign Disclosure Office that information being accessed by the FN is releasable. - A copy of the accreditation statement by the local DAA. - A proposed solution that explains how access by the foreign national will be limited to only information determined releasable by the Foreign Disclosure Office. 8. Once access is approved, C&A documentation must be updated and the DAA representative must concur with updated changes. 9. E-mail account mailbox display names for foreign nationals must include the designation "FN" included in the Rank field, so people know they are sending or receiving e-mail to or from a foreign national (i.e. "CIV/FN", "MAJ/FN", etc) 10. Significant changes, such as a new requirement for access to a different type of data, a different nationality filling a position or billet, etc, require the above steps to be re-accomplished.
B. FN civilian employed directly or indirectly by the US Government in accordance with SOFA, whose job includes duties as a Functional System Administrator (FSA)	Same requirements as A. Must meet other requirements for FSAs (training, etc). FNs are not authorized to be FSAs for sensitive or critical information systems such as command and control systems, or financial systems controlling funds greater than $10 million. Duties as FSA must be included in the C&A package.
C. FN civilian employed directly or indirectly by US Government in accordance with SOFA, whose job includes duties as a Workgroup Manager (WM)	Same requirements as B.
D. FN in coalition position or billet	Same requirements as A., but PACAF/CV must certify that access to the information is required for job performance. No provision for FSA or WM duties.
E. FN military member in Defense Personnel Exchange Program (DPEP) position or billet	Same requirements as A, but because it is a US position or billet the Wing Commander can approve access. Package must still be routed via PACAF/FDO (Foreign Disclosure Office) first.
F. FN military member in DPEP position or billet whose job includes duties as a FSA	Same requirements as B, but because it is a US position or billet the Wing Commander can approve access. Package must still be routed via PACAF/FDO first.

G. FN military member in DPEP position or billet whose job includes duties as a WM	Same requirements as C, but because it is a US position or billet Wing Commander can approve access. Package must still be routed via PACAF/FDO first.
H. FN Contractor	Same requirements as A. The Contract/Statement of Work (SOW) must state why access by the contractor is required, and that the NAC or equivalent check on the FN contractors is required.
I. FN Contractor in position or billet whose job includes duties as an FSA or WM.	Same requirements as B. The Contract/Statement of Work (SOW) must state why access by the contractor is required, and that the NAC or equivalent on the FN contractors is required.
J. FN member of a civilian organization supporting humanitarian operations	Same requirements as A., but verification that access to the information is required for job performance must be made by the DAA for the contingency/ operation (i.e. JTF commander. If none has yet been appointed/determined, then the DAA will be the HQ PACAF/SC). No provision is made for FN members of civilian organizations supporting humanitarian operations to perform FSA or WM duties.
K. FN student, military or civilian, requiring access to a campus LAN	1. Due to the high turnover of students and short duration of some courses, as well as the limited and specific information available to the student, the requirements for access are met with slightly different procedures. 2. Determine the exact information, business and common-user applications accessible by students (e-mail, specific web-sites, specific shared folders, specific software/data, notes, course materials, etc). Determine all nationalities of students likely to attend the course/school. Unit commander must certify that access to the information is required for job performance and is directly beneficial to the US government, and that only nationalities listed will have access. 3. PACAF Foreign Disclosure Office will determine the releasability of information to the foreign nationals listed based on the information provided at item 1, and will provide a release statement based on all the nationalities and information available to them. Access is not allowed to any unclassified information system or website containing information that is controlled under the Arms Export Control Act, the Privacy Act, and exemptions to the Freedom of Information Act unless it is approved by the system DAA/website owner and the local Foreign Disclosure Officer. 4. To satisfy the user-training requirement, all students must sign an agreement listing the same restrictions and conditions for use found in the current user licensing training course to include the consequences of abuse (immediate dismissal from the course/school).

	5. All personnel, including FNs, must have a NAC or equivalent performed prior to access to any unclassified IS IAW AFSSI 5027 and AFI 31-501. Foreign nationals require host government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government; and a Defense Clearance and Investigations Index (DCII) Check; and an FBI-HQ/ID where information exists regarding residence by the foreign national in the United States for one year or more since age 18. For foreign nationals attending a course of instruction for a limited period this requirement can be met by forwarding a Security Clearance Verification letter with an organizational letterhead from the student's security office or organization to the Unit Security Manager for the school. The letter must include the student's full name, date and place of birth, rank, occupation or employment activity, current security clearance and date of clearance, and a POC and contact information. 6. WM and SA duties will only be performed by US personnel. 7. PACAF/CV is the lowest authority able to approve access by foreign nationals to any PACAF controlled unclassified sensitive information IS. In addition to the above, the request package must include: - A brief mission statement and description of current environment. - Organizations involved and POCs. - Specific information and applications required (E-mail, specific business application, specific web sites and/or pages, etc). - What and how often information will be transmitted. - Determination by the MAJCOM Foreign Disclosure Office that information being accessed by the FN is releasable. - A copy of the accreditation statement by the local DAA. - A proposed solution that explains how access by the foreign national will be limited to only the information determined to be releasable by the appropriate foreign disclosure office. 8. Once access is approved, C&A documentation must be updated and the local DAA must concur with updated changes. 9. If e-mail accounts are used, mailbox names for foreign national students must include the designation "FN Student" following the account name, so people know they are sending or receiving e-mail to or from a foreign national (i.e. "Student22 FN Student 5 AF/SC …" or "Last-name First-name Rank FN Student JP 5 AF/SC …"). 10. Significant changes, such as a new requirement for access to a different type of data, a new nationality attending the school/course, etc, require the above steps to be re-accomplished.

REMARKS

1. A Foreign National is defined as anyone who is a non-US citizen, regardless of any other status.

2. Not all Foreign National (FN) status and access types can be encompassed in the above table, but most cases are listed, and these can be used as a guide for other cases. When in doubt, use the requirement with the highest-level of security - access should be allowed where absolutely needed, but only when security requirements are met. Contact the Wing or MAJCOM IA office for further guidance.

References:

AFI 33-202, paragraphs 3.7 thru 3.7.2 and 3.7.6.

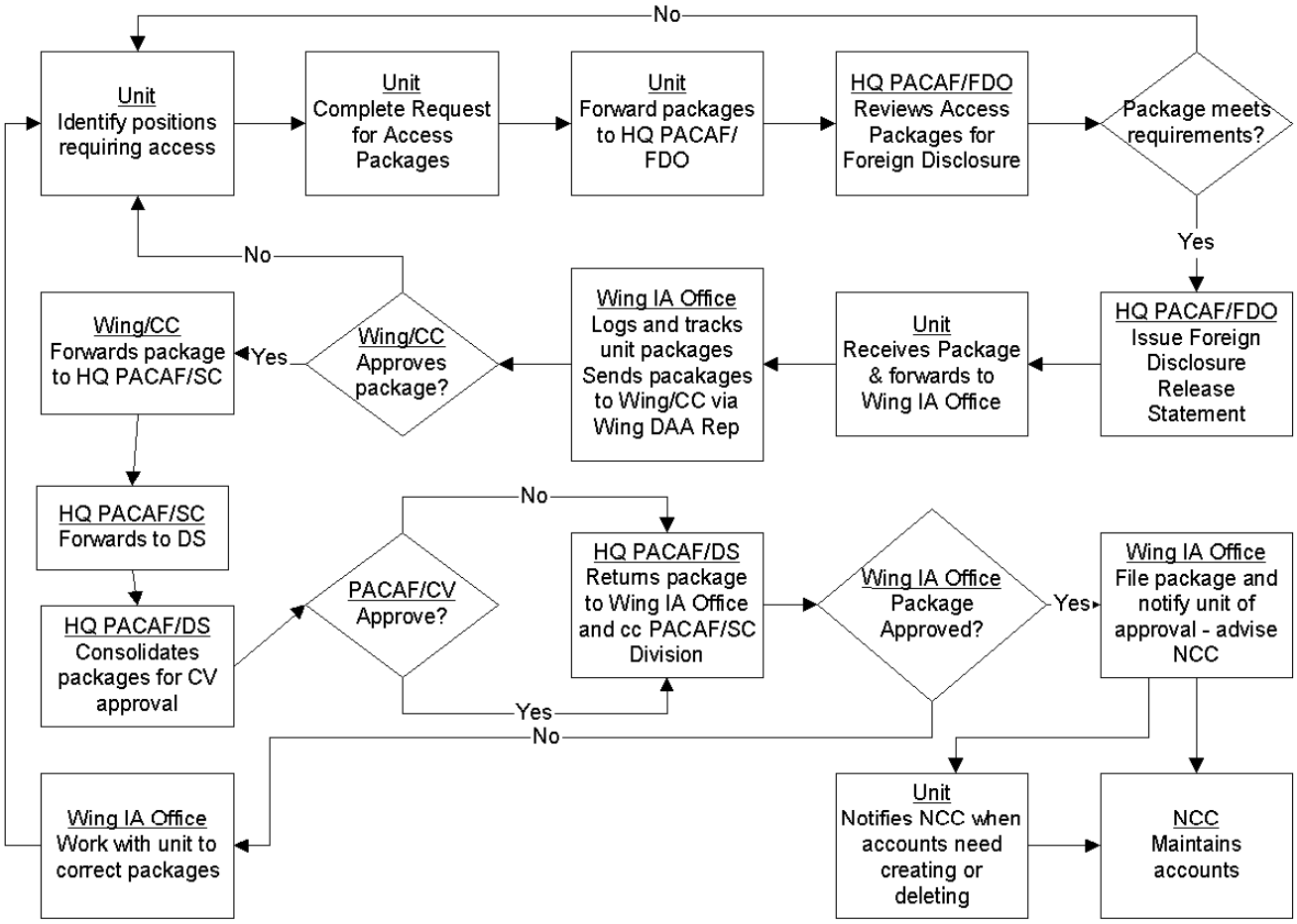
AFI 31-501, table A3.2, rule 4.

DOD Publication 5200.2-R.

CJCSI 6740.01

Attachment 12(Added)

FOREIGN NATIONAL ACCESS APPROVAL PROCESS FLOWCHART



RONNIE D. HAWKINS JR., Colonel, USAF
Director, Communications and Information