BY ORDER OF THE COMMANDER
PACAF REGIONAL SUPPORT CENTER

PACAF REGIONAL SUPPORT CENTER
INSTRUCTION 31-113

22 MARCH 2024

Security

INSTALLATION ACCESS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading on the e-Publishing website at **www.e-Publishing.af.mil**.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 611ASUS/SFM

Certified by: 611ASUS/CC
(Maj Joshua P. Caskey)

Supersedes: JBELMENDORF-RICHARDSONI31-1130, 5 June 2018

Pages: 19

This instruction implements Department of Defense Manual (DoDM) 5200.08 Volume 3_Air Force Manual (AFMAN) 31-101 Volume 3, *Installation Perimeter Access Control,* and Department of the Air Force Instruction (DAFI) 31-101, *Integrated Defense,* and is used in conjunction with Air Force Tactics, Techniques, and Procedures (AFTTP) 3-4.31V1, *Area Security Operations*, and the Internal Security Act of 1950, to establish entry control procedures and policies for all areas controlled by Pacific Air Forces (PACAF) Regional Support Center (PRSC). This instruction applies to all personnel, military, civilian and contractors, entering or transiting PRSC installations to include National Guard and Reserves. Ensure all records generated as a result of processes prescribed in this publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with (IAW) the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Submit requests for waivers through the chain of command to the publication office of primary responsibility (OPR) for non-tiered compliance items. This instruction cannot be supplemented or further extended. Refer recommended changes and questions about this publication to the OPR, using Department of the Air Force (DAF) Form 847, *Recommendation for Change of Publication*. Route the DAF Forms 847 through the appropriate chain of command. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force. This publication requires the collection and maintenance of information protected by Title 5 United States Code (USC) Section 552a, *Records Maintained on Individuals* "*Privacy Act of 1974"*. Collected information is considered Controlled Unclassified Information. Authorization to collect

information is 10 U.S.C. 9013, *Secretary of the Air Force*; Department of Defense (DoD) 5200.08-R, *Physical Security Program*; and E.O. 9397, *Numbering System for Federal Accounts Relating to Individual Persons*, as amended. The applicable Privacy Act System of Records Notice (SORN), F031 AFMC C, *Automated Installation Entry Control System/Visitor Center Records* (July 9, 2010, 75 FR 39500), can be found at **http://dpclo.defense.gov/Privacy/SORNs.aspx**. Request to release Privacy Act information to persons or agencies outside the DoD must be done in accordance with AFI 33-332, *Air Force Privacy Act and Civil Liberties Program*.

SUMMARY OF CHANGES

This instruction is substantially revised and must be completely reviewed. Changes made include updates to correlate with new policies and procedures and updated terminology.

1. Overview. This instruction establishes access control procedures to restrict and control entrance to installations to authorized personnel in order to protect personnel, resources, and missions.

1.1. The Pacific Regional Support Center Commander (PRSC/CC) is the Installation Commander, responsible for installation and logistics support of remote, austere sites and airfields across the Pacific area of responsibility and include the following sites:

1.1.1. Eareckson Air Station, Wake Island Airfield, and King Salmon Airport.

1.1.2. 3 Hawaii sites: Ka'ala Air Force Station, Koke'e Air Force Station, and the Pacific Air Defense Sector (PADS) on Wheeler Army Airfield.

1.1.3. 15 Alaska Radar System (ARS) Long Range Radar Sites (LRRS): Barter Island, Cape Lisburne, Cape Newenham, Cape Romanzof, Cold Bay, Fort Yukon, Indian Mountain, King Salmon, Kotzebue, Murphy Dome, Oliktok, Point Barrow, Sparrevohn, Tatalina, and Tin City

1.1.4. 3 Radio Relay sites Middleton Island, St. Paul Island, and Valdez.

1.2. Access modes vary per site and physical location.

1.3. IAW DAFI 31-101, all U.S. Air Force installations are designated "CLOSED" installations, to include PRSC installations. All personnel must have specific permission to enter the installation, possess the appropriate credentials, and be vetted through an authoritative government database to ensure fitness to enter the installation.

1.4. The Pacific Air Forces (PACAF), PRSC/CC exercises the authority to publish and enforce command or installation-specific guidance and procedures for safeguarding personnel, facilities, and property. This authority is derived from the Internal Security Act of 1950, DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, DoD 5200.08-R, and this instruction.

1.5. Installation perimeter access control procedures include identity proofing, fitness determination vetting, and issuance of access credentials.

1.6. The Protection of Civil Liberties, Privacy, and Personally Identifiable Information (PII) collected and utilized in the execution of this instruction must be safeguarded to prevent any unauthorized use, disclosure, or loss, IAW the requirements of*;* DoD 5400.11-R, *Department of Defense Privacy Program;* and AFI 33-332, *Air Force Civil Liberties and Privacy Program*.

1.7. The standards prescribed herein are the minimum required for PRSC installations.

2. Roles and Responsibilities. The integrated defense program belongs to the PRSC/CC IAW DAFI 31-101.

2.1. The PRSC/CC, in alignment with DoD, Service Component, Combatant Command (CCMD), combined joint forces command, and Major Command (MAJCOM) policies, will:

2.1.1. Identify specific procedures for access credential issuance on the installation. This includes rules associated with identity proofing, vetting, and fitness determination, credential issuance (form of temporary credentials) or denial, access control operations/screening, periodic re-vetting of identities, and vehicle and container searches, as applicable.

2.1.2. Implement procedures for off-base first responders' physical access requirements during emergencies.

2.2. Unit Commanders, tenant Unit Commanders, Agency Chief or equivalent Staff Agency Chief must ensure their personnel understand and follow access control guidance and procedures as outlined in this instruction.

2.3. PRSC/CC has delegated, 611th Air Support Squadron Security Forces Manager (ASUS/SFM) as the OPR responsible for identity proofing, vetting, and determination of fitness and access authorizations and privileges. The 611 ASUS/SFM will:

2.3.1. Serve as the Installation Commander's primary advisor for installation access control.

2.3.2. Conduct access control assessments and planning.

2.3.3. Develop and codify installation access control policies in the Integrated Defense Plan and this instruction.

2.3.4. Vet personnel submitted by 611th Air Support Squadron Project Manager (ASUS/PM) and PRSC Detachment (Det) 1 and Det 2 personnel prior to issuance of an approved Site Arrival Request (SAR). A log of all personnel vetted will be kept.

2.3.5. Track, package, route, and serve all Debarment packages through the 11th Air Force Judge Advocate (AF/JA), 611th Air Support Squadron Commander (ASUS/CC), and the PRSC/CC.

2.3.6. Track and vet personnel requesting firearms and maintain a list of approved firearms on each ARS site to include arrival and departure dates of firearms.

2.4. The sponsoring government agency is responsible for identifying personnel, mission needs, and time-definite access information for non-government personnel who request site access.

2.5. Contractors are responsible for identity proofing and vetting their personnel, entering validated employee data into the SAR, certifying employees meet eligibility requirements IAW Federal Acquisition Regulation (FAR) 22.1802 and Air Force FAR Supplement (AFFARS) 5352.242-9000, *Contractor Access to Air Force Installations,* updating employee information, and ensuring employees are aware of the requirement to maintain possession of approved access credentials at all times.

2.6. PRSC Det 1 and 2 are responsible for maintaining the Wake Island/Eareckson Air Station security access programs, with coordination from 611 ASUS/SFM and 611 ASUS/PM, to include all training and credentialing to operate as peace officers (Det 1 only) IAW with Title 32, Code of Federal Regulations (CFR), Part 935, *Wake Island Code*, as appointed by the PRSC/CC. PRSC Det 1 and Det 2 are also responsible for ensuring that all personnel have been appropriately vetted by the 611 ASUS/SFM. Unannounced arrivals, emergency landings, Gas-n-Go flights who Remain Over Night (RON), or persons arriving who have not been vetted, will be met by Detachment personnel who will positively identify the individual by performing a 100% hands-on identification check ensuring authenticity of credentials, verify the purpose of installation access, and collect all required information for immediate vetting by 611 ASUS/SFM.

3. Requirements for Access to PRSC Installations.

3.1. All personnel will be granted unescorted access to PRSC installations upon appropriate vetting by 611 ASUS/SFM. Note: Vetting for access to PADS on Wheeler Army Airfield will be conducted by Directorate of Emergency Services, Visitor Control Center. Foreign military visitors to PADS on Wheeler Army Airfield sites must be vetted by PACAF/A2 Foreign Disclosure Office.

3.2. Unescorted access requires individuals to establish their identity, establish an acceptable purpose for presence on the installation, and undergo fitness determination IAW DoDM 5200.08V3_AFMAN 31-101V3.

3.3. The SAR is a multi-use document and will be used to request access to all PRSC installations.

3.3.1. In order to ensure proper identity proofing and vetting is accomplished, all personnel requesting to access PRSC installations are responsible for completing the SAR in its entirety. Full name, including middle initial, date of birth, gender, entire social security number, current/valid driver's license, (include state of issue and driver's license number with all letters and numbers), DoD ID Number as applicable, and current clearance must be annotated in their appropriate places. **Note:** Failure to complete all required information will delay the vetting process, and the form will be returned to the Submitting Contractor, Government Entity, or individual submitting the SAR, until the appropriate information is submitted.

3.3.2. State-issued Driver's Licenses and Identification Cards **must** be "REAL ID" compliant IAW Department of Homeland Security policy, to access Federal Installations and Facilities." If the issuing state's compliance deadline has been extended, then that credential may be used until the extension date. The most current information on state compliance may be found at **https://www.dhs.gov/real-id**.

3.3.3. All personnel requesting access privileges will be vetted on a trip-by-trip basis.

3.3.3.1. Due to contract constraints, ARCTEC Alaska personnel do not submit SARs. Periodic vetting of personnel will take place throughout the year.

3.3.4. In order to complete vetting and identity proofing in a timely manner, **all SARs must be received by the 611 ASUS/SFM office no later than 14 days prior to the travel date.** Failure to provide the SAR 14 days prior may result in delay or denied travel and requester will need to resubmit for a future travel date. Foreign Nationals requesting travel to a site must submit, the SAR, colored digital copies of their Passport and/or Permanent Resident Card to the 611 ASUS/SFM office no later than 45 days prior to travel or travel will be denied. **Note:** On a case-by-case basis, mission critical requests for short notice travel will be reviewed and approved by the 611th Air Support Squadron Director of Operations (ASUS/DO).

3.3.5. Authorized credentials used for PRSC installation access will be IAW, DODM 5200.08v3_AFMAN 31-101v3, and this instruction. The following are Authorized Credentials for Access to PRSC installations, with an approved SAR:

3.3.5.1. Department of Defense (DoD) issued Common Access Card (CAC).

3.3.5.2. "REAL ID" compliant driver's license or non-driver's identification card issued by a State, territory, possession, or the District of Columbia.

3.3.5.3. Enhanced driver's license issued by a State, territory, possession, or the District of Columbia.

3.3.5.4. United States passport or passport card.

3.3.5.5. Foreign passport bearing an unexpired immigrant or non-immigrant visa or entry stamp.

3.3.5.6. Active Federal, State, and Local law enforcement credentials are considered appropriate access credentials in performance of official duties. Due to time

considerations, law enforcement personnel may be allowed on PRSC sites without an approved SAR. **Note:** Notify 611 ASUS/SFM **immediately** when any law enforcement agency accesses PRSC installations.

4. Identification Check and Vetting Procedures.

4.1. Performance of the Identity Proofing, Vetting and Initial Fitness Determinations is delegated IAW DoDM 5200.08v3, AFMAN 31-101v3, to the 611 ASUS/SFM.

4.2. Identification will be physically (hands-on) cross-checked and validated against a 611 ASUS SAR Office or 611 ASUS/PM approved SAR by site personnel upon site arrival. Acceptable forms of ID are outlined above in **paragraph 3.3.5**.

4.3. All individuals requesting non-emergency access to any PRSC installation will be queried against the National Crime Information Center.

4.3.1. Personnel with a valid emergency or life threating scenario may enter PRSC installations for the length of the emergency or until other arrangements are made.

4.3.2. All emergency access will be IAW **paragraph 6.4**.

4.4. The following Non-DoD federal employees will be considered identity proofed and vetted when issued their agencies Personal Identity Verification (PIV) IAW DoDM 5200.08V3_AFMAN 31-101V3: Dept. of State, Dept. of Treasury, Dept. of Justice, Dept. of the Interior, Dept. of Agriculture, Dept. of Commerce, Dept. of Labor, Dept. of Health and Human Services, Dept. of Housing and Urban Development, Dept. of Transportation, Dept. of Energy, Dept. of Education, Dept. of Veterans Affairs, Dept. of Homeland Security, and the United States Postal Service.

4.5. Any barge supporting PRSC installations must submit a SAR. All barge companies must submit a SAR 30 days prior to setting sail to conduct contract operations. Once approved, site personnel of arriving barge crew and ships are subject to undergo search or identity checks as determined by 611 ASUS/SFM, site personnel, or Force Protection Condition (FPCON). Crew members without an approved SAR must remain on the barge unless an emergency arises in which case they shall be escorted if they are required to leave the pier area.

4.6. Civilian aircraft and ships are not permitted to land or shore at any PRSC installation without a valid emergency reason or an approved Prior Permission Request (PPR). If an emergency exists, the 611 ASUS/SFM and 611 ASUS/PM shall be notified as soon as possible IAW the Installation Commander's critical information requirement. All personnel will remain on their vessels until the Installation Commander releases them or proper vetting can take place by 611 ASUS/SFM.

4.7. Contracted aircraft may land at PRSC installations with an approved PPR. All aircrew and passengers who remain in lodging or intend to receive base access must possess an approved SAR and be vetted IAW this instruction.

4.8. Military Aircraft comprised of Active Duty, Guard, Reserve and/or DOD Civilians, making fuel stops "gas and go" will not be required to submit a SAR. SAR is required if the gas and go becomes a RON. All Other aircraft will be required to complete the SAR process in its entirety. Full name, including middle initial date of birth, gender, entire social security number, a current/valid driver's license number (all letters and numbers) and state, and DoD ID Number, as applicable, and proper clearance must be annotated in their appropriate places.

Failure to completely annotate all information will delay the vetting process, and the form will be returned to the requester until the appropriate information is submitted.

4.9. Lost or injured personnel who appear at any PRSC installation shall be reported to the 611 ASUS/SFM and 611 ASUS/PM as soon as possible.

4.9.1. If personnel are injured, render first aid immediately, then notify 611 ASUS/SFM and 611 ASUS/PM at the first opportunity.

4.9.2. Site personnel will secure any weapons IAW **paragraph 8.4** of this instruction.

5. Installation Debarment.

5.1. Under the authority of the Internal Security Act of 1950, Department of Defense Manual 5200.8v3_AFMAN 31-101v3 and DAFI 31-101, PRSC/CC an Installation Commander may deny an individual access for involvement in the commission of a criminal offense when access is inconsistent with the interests of national security, or when access adversely affects the health, safety, or morale of personnel on that installation. Commanders may not delegate this authority.

5.2. Actions to debar contractors will be coordinated with the 611 ASUS/PM and contracting office.

5.3. Requests for debarment are based on facts and will be adjudicated on a case-by-case basis. The debarment order and supporting documentation will be routed through the 611 ASUS/SFM to the 11 AF/JA office for legal review and forwarded to the Installation Commander for final determination/approval.

5.4. Debarment determinations are made by the Installation Commander. The length of the debarment must be included in the notification.

5.5. Documentation supporting debarment orders will be kept on file with 611 ASUS/SFM for the period of the debarment.

5.6. Installation commanders may deny access and issuance of access credentials based upon information obtained during the vetting process that indicates the individual may present a threat to the good order, discipline, and morale of the installation.. Any person found to have an active want/warrant will be denied access to the site and local law enforcement will be notified. Personnel with an active warrant out of another state that do not have extradition orders will be denied access until the warrant is cleared through the National Crime Information Center. All other advisory notices, notices of probation status or other disclosures will be evaluated on a case-by-case basis. Denial rebuttals will be referred to the Installation Commander for final access determinations.

5.7. Upon notification of a flag during the Interstate Identification Index, the applicant's information will be compared to the fitness determination criteria matrix (**Attachment 2**) for recommendation for issuance of a debarment order from the Installation Commander.

5.7.1. At no point in time will information from a criminal background check be disseminated to the subject or anyone not authorized to receive the information. All requests for personally identifiable information from individuals under this provision will include a Privacy Act notice.

5.7.2. Offenses cited in the fitness determination matrix (**Attachment 2**) are examples of behavior that may pose a threat to the good order and discipline of PRSC installations. **Note:** This list is not all inclusive as there may be offenses or circumstances not listed that pose a threat and could be a potential debarment. If this occurs, 611 ASUS/SFM will route packages accordingly with their recommendation. Final determination will be made by PRSC/CC.

5.8. Individuals denied access via a debarment order may appeal debarment by providing any mitigating circumstances surrounding their case to the Installation Commander through the 611 ASUS/SFM for a final determination concerning base access privileges.

5.8.1. Debarment orders will be submitted by the 611 ASUS/SFM to contractors via certified mail or the DoD SAFE (**https://safe.apps.mil/**) safe access file exchange, where available, when a ".mil" email address is not accessible. Every attempt to send debarment orders to the address provided by individuals will be made, however that individual will still be barred whether or not they have received the order.

5.8.2. The 11 AF/JA will complete a legal review and brief the Installation Commander for final determination. The denial or approval authority is the Installation Commander.

5.9. Debarment Listing. The 611 ASUS/SFM will maintain a list of personnel barred from the installation.

5.9.1. All debarment/revocations will be delivered to all Program Managers and SAR office personnel on a quarterly or as needed basis. Each installation shall receive a copy of the Barment listing from the appropriate Program Manager.

5.9.2. 611 ASUS/SFM will make contact with 673d Security Forces Squadron Base Access (SFS/S5PD) and ensure personnel information is loaded into Defense Biometric Identification System (DBIDS) immediately following changes to ensure handheld scanners identify barred personnel at all installation entry control points in the attempt an individual attempts access to any other installation.

5.10. Barred at Another Installation. Individuals identified with a DBIDS status of "Barred" from an installation other than PRSC will be denied access to any PRSC installation.

6. Authorized Escorting. All approved personnel accessing PRSC installations must have a determined escorted or unescorted restriction annotated on the SAR.

6.1. Escort authority is inherent to all DoD military and civilian personnel.

6.2. Escort authority by site personnel is limited to personnel with a current Federal personal identity verification card.

6.3. Eligibility for escorting personnel in controlled and restricted areas will be determined by 611 ASUS/SFM and 611 ASUS/PM on a case-by-case basis.

6.3.1. 611 ASUS/SFM will work with owner/users to develop escort briefings that entail security and safety requirements. Escort briefings will be conducted before visitors are granted access to controlled or restricted areas.

6.3.2. Escort officials are responsible for the security and safety of all visitors. A single escort may escort no more than four visitors. Larger groups require additional escorts.

Escorts are required to maintain constant surveillance and control of visitors at all times in controlled or restricted areas.

6.3.3. Escort officials are required to positively identify individuals being escorted and are required to complete AF Form 1109, *Visitor Register Log*, before allowing access to restricted or controlled areas.

6.4. In the event of an emergency, site personnel must meet and escort responding personnel. Site personnel must be able to account for all responding personnel and equipment as they leave.

6.4.1. Emergency situations must be reported as soon as possible to the 611 ASUS/PM in accordance with the Installation Commander's critical information requirement. **Do not allow entry strictly on the use of flashing lights or sirens.**

6.4.2. During state-declared natural disasters, humanitarian aid in the form of shelter may be given at PRSC sites with approval of the Installation Commander.

7. Foreign Nationals.

7.1. Foreign nationals non-military are vetted by Det 631 Air Force Office of Special Investigations (AFOSI). Foreign military visitors to Hawaii sites must be vetted by PACAF/A2 Foreign Disclosure Office.

7.2. Entry onto PRSC installations by non-US personnel from countries designated by PACAF (**Attachment 3**) is not authorized without prior coordination with AFOSI and subsequent approval of the Installation Commander.

7.3. The authorized sponsor will use the established SAR process for access to PRSC installations. The request will be coordinated with the local Office of Special Investigations (OSI) office and 673d Security Forces Squadron (SFS) base access office before approval by the Installation Commander. See **paragraph 3.3** and related sub paragraphs.

7.4. Foreign military visitors for all PRSCC sites must be vetted by the 11th Air Force Foreign Disclosure Officer via the Department of State's Foreign Visit Request System.

8. Privately Owned Weapons at PRSC Installations.

8.1. Personnel assigned to ARS sites, including King Salmon Airport, permanently or in temporary duty status, are allowed privately owned weapons for personal protection from wildlife. One privately owned weapon per person may be allowed on ARS sites with 20 rounds of ammunition. Privately owned weapons will be considered on a case-by-case basis by the 611 ASUS/SFM. The 611 ASUS/SFM will vet individuals requesting to carry weapons on PRSC installations to ensure compliance with the Lautenberg Amendment to the Gun Control Act of 1968, effective 30 September 1996.

8.1.1. Alaska Department of Fish and Game, *The Essentials for Traveling in Alaska's Bear Country*, states *"If you are inexperienced with a firearm, it can be difficult to successfully deploy in emergency situations. Additionally, a wounded bear can be a greater threat to human safety. A .300-Magnum rifle or a 12-gauge shotgun with rifled slugs are appropriate weapons if you must shoot a bear. Heavy handguns such as a .44-Magnum may be inadequate in emergency situations, especially in untrained hands."*

8.1.2. Recommended weapons for personal protection from wildlife are rifles .300 Magnum or larger caliber, shotguns 12 gauge or larger with rifled slugs. Suitable, lower caliber long guns or handguns capable of stopping a charging animal, may be requested and will be approved on a case-by-case basis by the PRSC/CC or Designated Representative.

8.2. ARS contractors may request one additional weapon for hunting purposes off the installation. A maximum of 60 rounds of ammunition is allowed for hunting. All personnel will be vetted per **paragraph 8.1**.

8.3. Requests to carry privately owned weapon will be made during the SAR process and personnel must provide the following information: make/model/serial number/full caliber of weapon, completed Air Force Form 1314, *Firearms Registration*, and completed Department of Defense Form 2760, *Qualification to Possess Firearms*. Personnel must complete a national or state certified weapons safety course or hunter safety course with weapons safety as a component, either in person or on-line within the last 5 years. Proof of course completion will be provided to 611 ASUS/SFM prior to any weapons approval.

8.4. Personnel must store their weapons in the site weapons safe when not being utilized and sign out the privately owned weapon through the Site Manager. The Site Manager will limit access to the weapons container to him/her or their alternate. Personnel may not remain armed inside the lodging/food service area of the site for more than 10 minutes.

8.5. If a privately owned weapon is discharged while on the installation, the contractor must notify the 611 ASUS/PM and 611 ASUS/SFM as soon as possible. A written report outlining all actions and pertinent facts will be submitted to the above offices within 24 hours of the incident. Photographs, if available, will also be submitted to support the report. The PRSC/CC may appoint an investigating official.

8.6. Alcohol must not be consumed within 8 hours prior to arming. At no time will the site manager allow the individual to be armed if suspected of consuming alcohol within the prescribed time period. Responsibility rests with the Site Manager for enforcement.

8.7. Personnel must adhere to all Federal, State, and Local laws.

8.8. All personnel will read the Alaska Department of Fish & Game brochure "*Know Your Bear Facts, The Essentials to Travelling in Alaska's Bear Country"* and any contractor provided training on site.

8.9. Hunting is not allowed on PRSC installations and privately owned weapons used for this purpose must immediately be taken off the installation.

8.10. Personnel transiting through Joint Base Elmendorf-Richardson for transportation to/from PRSC sites must adhere to Joint Base Elmendorf-Richardson Instruction (JBELMENDORF-RICHARDSONI) 31-107, *Weapons Registration and Child Access Prevention Policy and* JBELMENDORF-RICHARDSONI 31-113*, Base Access Program.*

9. Government Owned weapons at PRSC Installations.

9.1. Government agencies may request to carry government-owned weapons via the SAR process, **paragraph 3.3** above. Requesting, storage, handling, and reporting procedures are the same as listed in **paragraph 8.4**. AFOSI is exempt from this requirement. Other Law

Enforcement Agencies requesting exemption from the procedures listed in **paragraph 8.4** will be considered on a case-by-case basis.

9.2. Requests from government agencies that require personnel to carry more than one weapon will be considered on a case-by-case basis.

10. Photography on PRSC installations and in Restricted Areas.

10.1. IAW DAFI 31-101, Photography inside controlled or restricted areas on PRSC installations is prohibited unless authorized by the PRSC/CC. Approval for authorizing photography is delegated to the 611 ASUS/SFM or Program Managers for the photographed area.

10.2. In all cases, photography in areas must adhere to the following guidance.

10.2.1. Photographer must be in possession of an approved SAR validated by the 611 ASUS/SFM approving the use of an electronic device equipped with camera owned by the government agency the employee is assigned to, or a company owned electronic device equipped with camera. Devices equipped with WiFi and/or Bluetooth are not authorized in classified open storage areas. **Note:** At no time will cell phones be authorized while in a restricted area or classified open storage areas on PRSC installations.

10.2.2. Photography in support of Quality Assurance program or incident reports are authorized. Images will be transferred by official means and then deleted once processed.

10.2.3. Personal photography or videography is limited to the residence and/or Morale, Welfare and Recreation (MWR) areas of the installation.

10.2.4. Personnel taking photos or video must be aware of their surroundings and what is being captured in the photo or video; limiting it to the specific items of interest and minimize exposure of critical assets, security measures or other Operational Security (OPSEC) concerns.

10.2.5. ALL personnel will be responsible to report unauthorized photos and videos to the site Manager, 611 ASUS/PM or the 611 ASUS/SFM.

11. Disclaimer. Entry control policy and procedures are subject to change at any time by direction of the Installation Commander. All permanent changes to this instruction will be done IAW Air Force publication policies outlined in DAFMAN 90-161, *Publishing Processes and Procedures.*

BREANNA D. FULTON, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

5 USC §552a, *Records Maintained on Individuals,* "*Privacy Act of 1974",* as amended

Internal *Security Act of 1950*

32 CFR Part 935, *Wake Island Code*

F031 AFMC C, *Automated Installation Entry Control System/Visitor Center Records* (July 9, 2010, 75 FR 39500)

DoD 5200.08-R, *Physical Security Program,* 09 April 2007

DoD 5400.11-R, *Department of Defense Privacy Program*, 14 May 2007

DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)*, 10 December 2005

DoDM 5200.08V3_AFMAN 31-101V3, *Installation Perimeter Access Control,* 27 February 2020

DAFI 31-101, *Integrated Defense*, 25 March 2020

AFFARS, *Air Force Federal Acquisition Regulation Supplement*

AFI 33-322, *Records Management and Information Governance Program,* 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

AFTTP 3-4.31V1, *Area Security Operations*, 16 August 2021

Directive Type Memorandum (DTM) 08-006, *DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12),* Incorporating Change 5, 8 October 2013

Homeland Security Presidential Directive-6, *Integration and Use of Screening Information*, 16 September 2003

Homeland Security Presidential Directive-11, *Comprehensive Terrorist-Related Screening Procedures*, 27 August 2004

Homeland Security Presidential Directive-12, *Policy for a Common Identification Standard for Federal Employees and Contractors,* 27 August 2004

Homeland Security Presidential Directive-24, *Biometrics for Identification and Screening to Enhance National Security*, 5 June 2008

FIBS PUB 201-2, *Personal Identity Verification for Federal Employees and Contractors,* March 2006

AFFARS 5352.242-9000, *Contractor Access to Air Force Installations*, 01 March 2023

PRSC IDP,

JBELMENDORF-RICHARDSONI 31-107, *Weapons Registration and Child Access Prevention Policy,* 28 December 2015

JBELMENDORF-RICHARDSONI 31-113, *Base Access Program*, 19 January 2023

FAR 22.1802

Alaska Department of Fish and Game, *Know Your Bear Facts, The Essentials for Traveling in Alaska's Bear Country,* July 2013

Prescribed Forms

None

Adopted Forms

DD 2760, *Qualification to Possess Firearms and Ammunition*

AF 1109, *Visitor Register Log*

AF 1314, *Firearms Registration*

Abbreviations and Acronyms

AFFARS—Air Force Federal Acquisition Regulation Supplement

AFMAN—Air Force Manual

AFTTP—Air Force Tactics, Techniques, and Procedures

ARS—Alaska Radar System

CAC—Common Access Card

CFR—Code of Federal Regulations

DAFI—Department of the Air Force Instruction

DBIDS—Defense Biometric Identification System

Det—Detachment

DoD—Department of Defense

DoDM—Department of Defense Manual

FAR—Federal Acquisition Regulation

FPCON—Force Protection Condition

IAW—In Accordance With

IDP—Integrated Defense Plan

LRRS—Long Range Radar Sites

MWR—Morale, Welfare, and Recreation

NCIC—National Crime Information Center

OPR—Office of Primary Responsibility

OPSEC—Operational Security

PADS—Pacific Air Defense Sector

PIV—Personal Identity Verification

PPR—Prior Permission Request

RON—Remain Over Night

SAR—Site Arrival Request

SFM—Security Forces Manager

SORN—System of Records Notice

Office Symbols

AF/JA—Air Force Judge Advocate

AFOSI—Air Force Office of Special Investigations

ASUS/CC—Air Support Squadron Commander

ASUS/DO—Air Support Squadron Director of Operations

ASUS/PM—Air Support Squadron Project Manager

ASUS/SFM—Air Support Squadron Security Forces Manager

CCMD—Combatant Command

MAJCOM—Major Command

OSI—Office of Special Investigations

PACAF—Pacific Air Forces

PRSC—Pacific Air Forces Regional Support Center

PRSC/CC—Pacific Air Forces Regional Support Center Commander

SFS—Security Forces Squadron

SFS/S5PD—Security Forces Squadron Base Access

Terms

Access Control—The use of physical and procedural controls to ensure only authorized individuals or items are given access to a facility or secure area.

Access Credential—A physical artifact issued by the Federal, State, or Local government that attests to one's right to credit or authority. The access credential contains and/or depicts characteristics, authorizations, and privileges for physical access and internal security controls.

Applicant—An individual requesting physical access to a facility and/or installation.

Cardholder—An individual possessing any RAPIDS issued ID card; PIV, CAC, or machine-readable IDs.

Control—As it relates to escorted personnel, control is defined as the ability to exercise restraint or direction of the escorted individual(s). It includes physical proximity of the sponsor except on-base residences. Sponsors do not have to be continuously present in on-base residences with their

escorts to ensure control as long as the escort stays within the residence or adjoining public (uncontrolled) areas.

Designated Official—The highest ranking official of the primary occupant agency of a Federal facility, or alternately, a designee selected by mutual agreement of tenant agency officials.

Escort Authority—Or sponsorship authority, it is the ability to sponsor or escort individuals on DoD installations.

Escorted Individuals—Personnel who require access, without determination of fitness, who must be accompanied by a cardholder with escort authorization. The escort requirement is mandated for the duration of the individual's visitation period.

Facility Security Level (FSL)—A categorization based on the analysis of several security-related factors, which serves as the basis for the implementation of physical security measures specified in ISC standards. Extended Definition: The five factors quantified to determine the FSL are: mission criticality, symbolism, facility population, facility size, and threat to tenant agencies, as well as additional intangible factors.

Federal Facility—Government leased and owned facilities in the United States (inclusive of its territories) occupied by Federal employees for nonmilitary activities.

Identity Proofing—The process of providing sufficient information (e.g., identity history, credentials, and documents) when attempting to verify or establish an identity for purposes of installation access.

Identity Registration—The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Identity Verification—The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

ID-based Access Control—Policies and practices requiring the presentation, inspection, and acceptance of a visitor's photo identification document for accessing a federal facility.

Knowledge-based Authentication—A method of authentication which seeks to prove the identity of someone using the knowledge of personal information associated with the asserted identity. It may use information sent to the individual in advance as part of the access control process or use answers to questions generated from a wider base of personal information (e.g., previous addresses) to which the agency has access.

PADS—Pacific Air Defense Sector.

Tier 1—A personnel security investigation combining a National Agency Check and written inquiries to law enforcement agencies, former employers and supervisors, references, and schools. All Tier 1 clearances conducted for the DoD shall include a credit check.

Restricted Area—A Federal facility (or part of a facility) only available to agency personnel, contractors, and their guests. Also referred to as Controlled, Limited, or Exclusion areas.

Semi-restricted Area—A Federal facility (or part of a facility) available to the general public but subject to ID-based access control.

State—One of 56 jurisdictions covered by the Act, which includes the 50 U.S. states, the District of Columbia, and the U.S. Territories of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, and the Commonwealth of the Northern Mariana Islands.

Sponsorship Government Authority—The sponsorship authority is the government program or project managers who have primary contracts with any PRSC units, or DoD mission partners that have been established as sponsorship authorities by the installation commander.

State-Issued Card—A REAL ID Act compliant driver's license or non-driver identification card issued by a state Department of Motor Vehicles or equivalent office. It does not include identification cards issued by other state agencies, such as an employee ID, hunting license, library card, or student ID.

Unescorted Individuals—Personnel who have been identity proofed and favorably vetted are eligible for unescorted access within the installation but are subjected to time-definite controls and restricted area limitations as appropriate.

Vetting—An evaluation of an applicant's or cardholder's character and conduct for approval, acceptance, or denial for the issuance of an access control credential for physical access via authoritative databases.

Attachment 2

FITNESS DETERMINATION MATRIX

Table A2.1. Fitness Determination Matrix.

PRSC FITNESS DETERMINATION MATRIX	
Offenses Preventing Installation Access	**Time Since Offense**
Current & Active Want/Warrant	Want/Warrant Current
Gang Member Validated by Law Enforcement	Validation Current
Unable to Verify Identity	Any inability
Illegal Immigrant	Validation Current
Debarred from any DoD Installation	At any Time
Appears on Federal Watch List for Criminal History or Suspected Terrorist Activity	At any time
Knowingly/Willingly Engaged in Acts to Overthrow U.S. government	At any time
Convicted for:	**Time Since Conviction**
Sexual Assault of Minor/Child Pornography	At any time
Espionage	At any time
Human Trafficking	At any time
Kidnapping	At any time
Manslaughter/Murder, to include attempted	At any time
Sabotage	At any time
Sexual Assault	At any time
Terrorism	At any time
Treason	At any time
Convicted of a Firearms or Explosive violation	At any time
Possession w/Intent to Distribute Marijuana or any other Controlled Substance	At any time
Armed Robbery/Burglary	At any time
Sex Offender (Registered/Failure to Register)	In past 20 years
Unarmed Robbery/Burglary	In past 10 years
All Violent Crimes Against Persons not covered	In past 10 years
Possession of Controlled Substance to include over 1 oz Marijuana	In past 5 years
Felony Aggravated Assault/Battery	In past 5 years
Arson	In past 5 years
Felony Larceny/Theft >$500	In past 5 years
Felony Possession/Use of Controlled Substance	In past 5 years
Felony DUI	In past 5 years

Simple Assault	In past 3 years
Domestic Violence	In past 3 years
DUI	In past 1 year
Criminal Trespassing	In past 1 year
Larceny/Theft <$500	In past 1 year

Note:

a. Personnel with pending criminal charges (i.e., hanging disposition) listed within this matrix may be denied access to PRSC Installations until final disposition of their criminal cases.

b. The conviction listing above is not comprehensive. The Installation Commander may deny access and issuance of access credentials based upon any information obtained during the vetting process that indicates the individual may present a threat to the good order, discipline, and morale of the installation.

Attachment 3

PACAF DESIGNATED COUNTRY LIST

Table A3.1. PACAF Designated Country List.

PACAF DESIGNATED COUNTRY LIST		
Country	**Country**	**Coun**
Afghanistan	Jordan	Qatar
Albania	Kazakhstan	Russia
Algeria	Kuwait	Saudi Arabia
Armenia	Kyrgyzstan	Singapore
Azerbaijan	Lebanon	Somalia
Bahrain	Libya	Sudan
Bangladesh	Malaysia	Syria
Belarus	Myanmar (Burma)	Taiwan
Bolivia	Moldova	Tajikistan
Bosnia	Morocco	Tunisia
Cuba	Nigeria	Turkmenistan
Egypt	North Korea	Ukraine
Georgia	Oman	United Arab Emirates
India	Pakistan	Uzbekistan
Indonesia	People’s Republic of China	Venezuela
Iran	Hong Kong	Vietnam
Iraq	Macau	Yemen
Israel	Palestinian Authority	