BY ORDER OF THE COMMANDER
502D AIR BASE WING

JOINT BASE PUBLICATION SAN ANTONIO INSTRUCTION 31-1131

16 AUGUST 2019

Security

INSTALLATION ACCESS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-publishing website at **www.e-publishing.af.mil** for downloading.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 502 SFG/S5

Certified by: 502 SFG/CC
(Col Jeffrey F. Carter)
Pages: 29

This instruction implements portions of AFMAN 31-113, *Installation Perimeter Access Control*, AFI 36-3026(I), *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members and Other Eligible Personnel*, and supports 502 ABW Plan 31-101, *Integrated Defense Plan (IDP).* Among other things, it assimilates portions of AFI 31-101, *Integrated Defense*, changes and it updates Joint Base San Antonio (JBSA) requirements from AFMAN 31-113, *Installation Perimeter Access Control*, and its AFGM2018-01 Apr 18, required to gain access to the installation and access procedures for International Military Students. This instruction outlines the use of the Defense Biometrics Identification Data System (DBIDS), encompasses identification card measures, outlines access procedures to Joint Base San Antonio and identifies Privately Owned Weapons policy. This instruction applies to all personnel, civilian and military, assigned, attached, visiting or accessing Joint Base San Antonio. This instruction requires the collection and maintenance of information protected by the Privacy Act of 1974 authorized by 10 USC. 8013, Secretary of the Air Force. System of Records Notice F031 AF SP O, *Documentation for Identification and Access Authority*, applies. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). Refer recommended changes and/or corrections to this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*, through your chain of command. Submit waiver requests to guidance in this publication to the OPR. This publication may be supplemented at any level, but all Supplements must be routed to the OPR of the publication for coordination prior to certification or approval. 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.

1. Overview.

1.1. JBSA Commander is responsible for installation support to 266 Mission Partners and Tenant Organizations across the area of responsibility. This instruction establishes access control procedures to restrict and control entrance to JBSA locations to authorized personnel to protect personnel, resources, assets and missions.

1.2. In accordance with Air Force Instruction 31-101, *Integrated Defense*, all US Air Force installations are designated as "CLOSED." Therefore, personnel must have specific permission to enter JBSA locations, possess the appropriate credentials and be vetted through authoritative Government databases to ensure fitness to access any area within JBSA. There are 29 installation access control points (ACP) or entry control facilities (ECF) amongst the five major locations which comprise JBSA (**Attachment 2**).

1.3. Access to all locations within JBSA is controlled. Access control procedures include identity proofing, fitness determination vetting and issuance of access credentials.

1.4. Daily identification checks of pedestrians and vehicle occupants are authorized at every JBSA Access Control Points or Entry Control Facilities. Additionally, identification checks may occur during higher Force Protection Conditions (FPCONS), Random Antiterrorism Measures (RAMs), alarm activations or as deemed appropriate by security forces personnel at any location within the installation.

2. Roles and Responsibilities.

2.1. The integrated defense program belongs to the Installation Commander in accordance with Air Force Instruction 31-101, *Integrated Defense*. Therefore, the Installation Commander has delegated to 502d Security Forces Group (SFG), as the OPR, the authority to enforce access control policy, guidance, regulations and applicable statutes with the authority and responsibility of the commander.

2.1.1. The 502 SFG will vet personnel submitted by Mission Partners or Tenants Organizations before issuance of an approved installation access pass or credential.

2.1.2. The 502, 802, and 902 Security Forces Squadrons (SFS) will maintain a list of on-installation privately-owned firearms.

2.1.3. The 502, 802, and 902 SFS will maintain a list of debarred individuals.

2.2. Organizations and units are responsible for identifying mission essential personnel and provide access information for DoD and non-DoD personnel to Security Forces.

2.3. The sponsor is responsible for providing the required information, in the proper format for their visitors requesting access. The sponsor is responsible and liable for the actions of their visitors while on the installation. It is prohibited to operate a cellular device while driving (you must use a hands free device). The speed limit on JBSA is 25 mph except where otherwise posted. Visitors are not allowed to bring weapons on to the installation, if you have a weapon, notify the installation access controller.

2.4. The visitors responsibility is to provide the required information, in the proper format for installation access. Abide by the laws of the installation to include, not operate a cellular

device while driving (you must use a hands free device), maintain the speed limit of 25 mph except where otherwise posted, and not bring a weapon on to the installation.

3. Authorized Credentials. As a closed installation, issuance of access credentials is limited to personnel with a valid requirement to access the installation. Access is granted to personnel with a valid and authorized access credential. Access credentials may be revoked at any time at the direction of the Installation Commander. During increases in FPCONs, supplemental identification may be required. Personnel are always required to carry authorized credentials while on the installation. Possession of authorized credentials does not provide inherent escort or sponsor authority. Personnel are subject to intermittent identification and credential checks as directed by the Installation Commander. Personnel must immediately report a lost or stolen access credential to the Security Forces Base Operations Center located at either Lackland, Fort Sam Houston, or Randolph.

3.1. Credentials must comply with the standards for installation access as directed by Air Force Manual 31-113, *Installation Perimeter Access Control, 2 February 2015* to be considered an authorized credentials (**Attachment 3**).

3.1.1. Authorized credentials include: Common Access Card (CAC), DD Form 2 (series) *United States Uniformed Services Identification Card* (Retired), *Armed Forces of the United States Geneva Conventions Identification Card* (Reserve), and *United States Uniformed Services Identification Card* (Reserve Retired), DD Form 1173, *Uniformed Services Identification and Privilege Card*, DD Form 1173-1, *Department of Defense Guard and Reserve Family Member Identification Card*, DD Form 2764S, *United States DoD/Uniformed Services Civilian Geneva Conventions Identification Card*, DD Form 2765S, *Department of Defense/Uniformed Services Identification and Privilege Card*, and DoD-Civilian Retiree Card.

3.2. While in the performance of official duties, Federal, Tribal, State, and local law enforcement officials with current police credentials (badge and department photo identification) may use those credentials for access. Emergency services personnel (police, fire, and emergency medical services) responding to an emergency may be allowed onto JBSA locations without proofing and vetting.

3.3. Individuals under 18 years of age, without a state-issued driver's license, state identification card or authorized credentials per AFMAN 31-113, may use a school record or report card, daycare or nursery school record or original/certified copy of a birth certificate issued by a state or territory of the United States as a credential for identity proofing and vetting.

3.4. Prohibited Use of Authorized Entry Credentials/Passes: Authorized credentials not issued for the specific purpose of engaging in commercial enterprise, are prohibited for use as commercial gain or to facilitate installation access for the purpose of furthering a commercial enterprise. Authorized credential holders are considered contractors or vendors for the purpose of entering a commercial/financial enterprise and must obtain approved contractor or vendor access credentials.

4. Identification Check and Vetting Procedures. Background checks authenticating an individual's identity and determining their fitness is a core principle of installation access control. Identity proofing is the process of providing sufficient information (e.g., identity history,

credentials and documents) when attempting to establish a person's identity. Individuals must appear at the Visitor Control Center (VCC) to be identity proofed and vetted. Identity Proofing Credentials are identified in **Attachment 3**.

4.1. Identification will be physically proofed, (hands-on) cross-checked and validated against authoritative databases. Performance of the vetting and initial fitness determination has been delegated per Air Force Manual 31-113, *Installation Perimeter Access Control*, Chapter 4, to the 502 SFG, 502 SFS, 802 SFS and 902 SFS.

4.2. Background Criminal history checks are mandated for all unescorted personnel requesting or requiring access to JBSA who are 16 years of age and older. This must include a National Crime Information Center (NCIC) check, Interstate Identification Index (III), terrorist screening database check, NCIC National Sex Offender Registry (NSOR), DOJ National Sex Offender Public Website (NSOPW), a check of the revocation and debarment roster and a Social Security Number (SSN) trace. For foreign contracts, additional checks such as the Department of Homeland Security E-Verify, U.S. visit and FVS-CM may be required. The requirement for this check must be written into the contract's statement of work.

4.3. A valid and unexpired driver’s license or identification card issued by a state or outlying possession of the United States provided it contains a photograph and biographic information such as name, date of birth, gender, height, weight, eye color and address, may be used for proofing and vetting purposes. Additionally, a Federal, State, or local Government-issued identification card provided it contains a photograph and biographic information such as name, date of birth, gender, height, weight, eye color and address may also be used.

5. Fitness Determination.

5.1. Debarments and any criminal history that pose a potential threat to the good order, discipline, or health and safety of the installation will incur an unfavorable fitness determination. Access will be denied to any person found to have an active want/warrant and the appropriate law enforcement agency will be notified. Personnel with an active warrant out of another state that does 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 determination.

5.2. Unescorted personnel access, without an authorized credential, must be vetted via NCIC Interstate Identification Index (III), the Texas Law Enforcement Telecommunication System (TLETS), and the Terrorist Screening Database (TSDB) for fitness of access. Additionally, background checks with local/government authoritative databases (e.g. Army Law Enforcement Reporting and Tracking System (ALERTS), Security Forces Management Information System (SFMIS), JBSA debarment, suspension and revocation systems) as required.

5.3. Information from a criminal background check will not be given to the subject or anyone not authorized to handle the information. Requests for personally identifiable information (PII) must follow the Privacy Act guidelines.

5.4. Offenses cited in the fitness determination criteria matrix (**Attachment 4**) are examples of behavior that may pose a threat to the good order and discipline of JBSA and are in no way all inclusive.

5.5. Individuals denied access via a fitness determination may provide mitigating circumstances surrounding their case to the Installation Commander, through the respective Security Forces Squadron (502, 802, or 902) for processing, within 10 days from the date access determination.

6. Authorized Escorting. Personnel accessing JBSA locations must have a determined *escorted* or *unescorted* restriction annotated on locally produced access credential. Escort authority is limited to personnel with a current Federal personal identity verification card per AFMAN 31-113.

6.1. Escort authority is inherent to all Department of Defense military, family members (age 18 an older) and civilian personnel with possession of an authorized access credential. Dependent minors 16 or 17 years of age (not legally emancipated) are authorized to escort minors of the same age or younger onto JBSA. Minors are not authorized to escort adults. **Note:** Foreign nationals may not be escorted at any time onto the installation without proper vetting through the Foreign Disclosure Office (FDO) (refer to paragraph 8 for specific information related to foreigner access).

6.2. Eligibility for escorting personnel in controlled and restricted areas will be determined by Installation Commander or owner/user of the area on a case-by-case basis.

6.3. DBIDS Card or pass holders **CANNOT** escort or vouch for personnel unless they have been granted escort authority and it is indicated on the DBIDS Card or pass. Escort approval authority for DBIDS card or pass is the 502 SFG/CC or designee. All requests seeking escort authority will be coordinated through the 502 SFG.

6.4. Trusted Traveler procedures may be used during FPCONs Normal through Bravo as local security conditions permit. The Trusted Traveler program is a local procedure allowing authorized personnel to escort family or personal guests traveling with the sponsor. Per the Directive-Type Memorandum 09-012 (reference (d)), sponsors present their identification for verification while simultaneously assuming responsibility for vehicle occupants. Trusted Traveler program is not applicable for those individuals who are requesting access to conduct business as a contractor, volunteer, subcontractor, service provider, vendor or supplier.

6.4.1. Personal guests are those visitors personally known and vouched for by the sponsor. By vouching for family or guest, the sponsor certifies all occupants meet acceptable documentation criteria for installation access in paragraph 5. **Note:** Foreign nationals may not be vouched/escorted at any time onto the installation without proper vetting through the FDO (refer to paragraph 8 for specific information related to foreigner access).

6.4.2. Trusted Traveler guests require an escort, unless they have a valid credential for entry, and must always remain with the sponsor until they depart from the installation. Members identified as the Trusted Traveler are responsible for their guests at all times. Individuals who are debarred or denied access cannot be escorted on the installation using the Trusted Traveler program. By accessing the installation, a debarred individual

could face criminal trespassing charges and escorts could lose escort and sponsor privileges.

6.5. The Installation Commander may suspend installation wide escort authority based on the local threat or may revoke escort authority privileges if a visitor is found on the installation without its escort. Additionally, suspension or termination of escort authority may occur if the escorted visitor violates law or regulation while on the installation while in the presence of the authorized escort. This suspension/termination authority is delegated to the 502 SFG/CC.

6.6. Installation bank/credit union employees with locally issued credentials are authorized to escort individuals onto their affiliated facilities within installation.

6.7. JBSA Independent School District school administrators, selected faculty members, and identified staff are authorized to escort individuals to the school that they work.

6.8. Privatized housing residents, with locally issued credentials, are authorized to escort individuals onto their affiliated installation housing area. **Note:** Non-military affiliated privatized residents must be 18 years or older to escort.

6.9. Escort authority privileges are automatically suspended at FPCON Charlie and Delta when the installation is postured for increased criminal or terrorist threats. FPCONs Charlie and Delta require more stringent access requirements and this program will not be in effect during these times unless otherwise approved by the 502 ABW/CC.

7. Authorized Sponsoring. Department of Defense military, family members (age 18 an older) and civilian personnel with possession of an authorized access credential have inherent authority to sponsor. Dependent minors 16 or 17 years of age (not legally emancipated) are not authorized to sponsor. Request for sponsorship for individuals without this inherent authority, must be requested to the 502 SFG for approval.

7.1. All sponsors must complete the JBSANANTONIO Form 7, *Unescorted Access Request* (UAR) to sponsor visitors onto the installation. This document is an "all-in-one" request. Sponsors will submit this document via an .mil email address to their local VCC (LAK: **lackland.vrc@us.af.mil**; FSH: **usaf.jbsa.502-abw.list.502-sfs-fsh-visitor-control-center-owner@mail.mil**; RND: **902sfs.vrc@us.af.mil**) requesting access to any location within JBSA for unaffiliated personnel who are not expected to be under full-time escort. It may be used to request a DBIDS card or pass, for a one or multiple day event. The following information will be provided for each visitor: sponsors information, proposed dates of visit, installation/facility to be visited, purpose of visit, visitor's name, date of birth, country of birth, identification type and state or country of issue. The document may be obtained on Air Force e-publishing at **www.e-publishing.af.mil** / publication+forms/ Forms / Bases / JB San Antonio / JBSanAntonio Form 7.

7.2. Active duty, Guard, 100% Disabled Veterans with DoD identification, Reserve military/retired personnel, or their dependents 18 years or older and civilian employees of JBSA, who have valid credentials to enter the installation unescorted, may sponsor visitors. Temporary Duty (TDY) personnel may sponsor someone onto the installation only through the duration of the TDY. **Note:** Foreign nationals with a valid CAC/Invitational Travel Order (ITO) are not authorized to sponsor any guests onto the installation that are not on their ITO to include U.S. nationals. (Refer to para 7.1 and para 8.)

7.3. Installation bank/credit union employees with locally issued credentials are authorized to sponsor individuals to the bank/credit union on their affiliated installation. (Refer to para 7.1 and para 8.)

7.4. JBSA Independent School District school administrators selected faculty members and identified staff is authorized to sponsor individuals to the school that they work. (Refer to para 7.1 and para 8.)

7.5. Privatized housing residents with locally issued credentials are authorized to sponsor individuals onto an installation they are affiliated with/assigned to, but sponsorship privileges should be limited to their particular housing area only. **Note:** Non-military affiliated privatized residents must be 18 years or older to sponsor. (Refer to para 7.1 and para 8.)

7.6. Inter-American Air Forces Academy (IAAFA). Permanent instructors assigned to IAAFA are authorized sponsorship privileges onto JBSA-Lackland only.

7.7. Defense Language Institute English Language Center (DLIELC) and IAAFA Students. DLIELC and IAAFA students do not have sponsorship privileges. Family members who accompany students must also be on ITO.

8. Foreign Nationals (Visitors). A "foreign national" is any person who is not a U.S. citizen or a person who is not a naturalized citizen. Persons with a U.S. 'green card' are considered a foreign national. They are lawful permanent resident aliens, who have a resident alien registration card (INS Form I-551), commonly known as a 'green card,' retain their foreign nationality and must be considered "foreign nationals." The terms "foreign national" and "alien" are used interchangeably. A person with dual citizenship, who is a citizen of the U.S. and another country may be treated exclusively as a U.S. citizen when in the United States.

8.1. Foreign Visitors will be processed per the guidelines established by the Installation FDO **(Attachment 5)**. Questions or concerns regarding foreign visitor processes should be addressed to the 502 SFG FDO.

8.2. Non-Official Foreign Visit/Guest. Foreign visitor/guest not on ITO, not documented in the FVS and traveling to any Joint Base San Antonio property in an unofficial capacity (i.e., family members and friends, contractors, etc.) will coordinate through the FDO, AFOSI and SFS ***10 days*** prior to arrival.

8.3. The authorized sponsor (U.S. Government Agency and/or CAC/DoD ID card holder) will complete and submit a JBSANANTONIO Form 7, *Unescorted Access Request* ***10 days*** prior to visit to the FDO email box at **502SRG.MAS.JBSA_ForeignRequest@us.af.mil**. The following information will be provided for each visitor: proposed dates of visit, installation/facility to be visited, purpose of visit, visitor's name, date of birth, country of birth, identification type and state or country of origin, i.e., passport number. The sponsor and foreign friend or family member will be processed for access at the applicable VCC if approved. The visitor must bring his/her identification credentials to the VCC. Once the visitor has been properly proofed and vetted, an Installation Access Pass for the duration of their visit will be issued. **Note:** JBSANANTONIO Form 7 may be obtained on Air Force e-publishing at **www.e-publishing.af.mil** / publication+forms/ Forms / Bases / JB San Antonio / JBSanAntonio Form 7.

8.4. Friends and family of foreign nationals are allowed to visit the foreign-member who is assigned or attached to JBSA under the following programs: Military Personnel Exchange Program (MPEP), Country Liaison Officer (CLO), and Guest Instructor (GI) will notify their host organization no later than ***15 duty days*** before the visit and request a pass for the duration of the expected stay. The Foreign member's organization (sponsor) will complete and submit a JBSANANTONIO Form 7, *Unescorted Access Request* ***10 days*** prior to visit to the FDO email box at **502SRG.MAS.JBSA_ForeignRequest@us.af.mil**.

8.5. For foreign visit questions or information concerning access, contact 502 ABW FDO at 210-652-5762 or email **502SRG.MAS.JBSA_ForeignRequest@us.af.mil** for guidance.

9. Credentialing Process .

9.1. The authorized sponsor (U.S. Government Agency and/or CAC/DoD ID card holder) will complete and submit a The JBSANANTONIO Form 7, *Unescorted Access Request* (UAR) for all installation access requests. Sponsors will submit this document via a .mil email address to their local VCC requesting access to any location within JBSA for unaffiliated personnel who are not expected to be under full-time escort. It may be used to request a DBIDS card or pass, for a one or multiple day events. The document may be obtained on Air Force e-publishing at **www.e-publishing.af.mil** / publication+forms/ Forms / Bases / JB San Antonio / JBSanAntonio Form 7 or search: *Unescorted Access-Request* or by contacting the appropriate VCC (**Attachment 6**) or by contacting the 502 SFG Access Control Manager at (210) 652-5751.

9.2. The use of DBIDS is mandated. Note: A DBIDS paper pass will be issued for access onto the installation for 180-days or less. For access greater-than 180-days a hard plastic DBIDS card will be issued for up to one year. DBIDS is the primary method for producing local visitor passes/cards on JBSA. If DBIDS is not available, a SFMIS pass will be issued; if SFMIS is not available, an AF Form 75, Visitor Pass will be issued.

9.3. Credential Issuance. Upon proofing, vetting, and determination of fitness, individuals must have a valid need for access and be properly sponsored. A DBIDS credential (paper or badge) will be issued. If DBIDS or SFMIS is available, AF Form 75 will be used.

9.4. Requests for access credentials must be made in person or via an encrypted .mil email address. The following information is required.

9.4.1. Sponsor's Full Name, DoD ID Number, organization, duty phone, times/dates/location and reason for the visit.

9.4.2. Applicant's full name, DOB, country of birth, driver's license number and state, or passport number.

9.4.3. If driving onto the installation, the applicant must provide proof of registration and insurance.

9.5. The following categories or individuals may be authorized an access credential:

9.5.1. Civil Air Patrol (CAP) Volunteers. CAP will provide an Entry Authorization Listing (EAL) with all cadets and parent/guardians needing access to the installation.

9.5.2. Veterans Administration (VA) Patient Access. Access is determined by a Veteran's Affairs appointment list that is forwarded by the TRICARE Operations and

Patient Administration (TOPA) organizational box to the affected VCC organizational box via the government network.

9.5.3. Privatized Housing Residents. Residents may be authorized access with limited escort and sponsor authority.

9.5.4. Contractors and vendors. Individuals or organizations that provide services to the installation may be issued an access credential. Foreign nationals are not authorized entry without processing through the FDO.

9.5.5. Honorary Commanders and Official guests. To build partnerships with local community leaders the 502 ABW/CC adopts certain programs allowing the credentialing of certain non-DoD members.

9.5.6. Gold Star Family Program. Members can be issued DBIDS credential as they are sponsored through the Air Force Families Forever (AFFF) program. AFFF will provide qualifying family members a memorandum authorizing the issuance of an access credential.

9.5.7. Civilian Students. Civilian personnel with no DoD affiliation attending classes on the installation through an on-the-installation college or university may be issued an access credential. Registration documentation is required.

9.5.8. JBSA Independent School Districts (ISD) Administrators. A limited number of ISD employees and administration personnel are authorized access credential with limited escort and sponsor authority.

9.5.9. Taxis/On-Demand Car Services. Yellow Cab & Town Cars are the only sponsored through the Army Air Force Exchange Service (AAFES) and are issued DBIDS Cards after proper vetting and ID proofing.

9.5.10. VIA/STAR Shuttle (Handicap Transport). Curbside vetting will be conducted by the ACP controller. Request the driver's license and conduct an NCIC check. If the response to the NCIC check is clear, the bus/shuttle will be authorized to proceed. If negative fitness information is revealed, deny access to the bus/shuttle and driver. Note: Curbside vetting will be suspended in FPCON Charlie or higher.

9.5.11. FEDEX, UPS, DHL, USPS. Package/mail delivery and pick-up service is a daily operation. Personnel under this category will require a sponsor, be proofed/vetted and issued an access credential not to exceed six months.

9.5.12. Designated Agent Program. These individuals provide caregiver support for active or retired military member, spouse or dependent child, which otherwise would not have access to the installation. These individuals provide "assistance" to the ID card holder.

9.6. An EAL is used for one time access for multiple visitors attending a sponsored event. An EAL will be completed for 10 or more visitors. EAL will be provided to all Access Control Points that have been preapproved to allow access of EAL individuals.

10. Military Training Graduations.

10.1. An organization hosting a graduation event must have its students prepare a JBSANANTONIO Form 7 immediately upon arrival. Each student is authorized to sponsor up to 10 visitors. Within the first two weeks of the students' arrival, the hosting organization cadre will submit the visitor request for vetting/processing. Once the list is cleared, and not later than four weeks before graduation, passes or denial documents will be provided to the organization's cadre. It is the responsibility of the hosting organization and the students to provide the passes to their visitors. Below are additional procedures for Lackland and Fort Sam Houston.

10.1.1. Lackland. Basic military training (BMT) students initiate their graduation guest lists upon arriving at their Military Entrance Processing Station (MEPS). Cadre will forward the required documents to 802d Security Forces Pass and Identification Section within the first two weeks of basic training. Students are provided the installation access passes for all cleared guests and denial letters (without derogatory information) uncleared guests.

10.1.2. Fort Sam Houston. Cadre will forward the required documents to 502d Security Forces Visitor Center within the first two weeks of training. Students are provided the installation access passes for all cleared guests and denial letters (without derogatory information) uncleared guests.

10.2. Guests are required to have their pass in their possession at all times while on the installation. Guests that forget their pass must be processed through a VCC for proofing and vetting before being allowed access onto the installation.

10.3. For additional information on access to graduations contact the 502d Security Forces Group Access Control Manager at 210-652-5751 or contact any of the VCC in Attachment 3.

11. Privately Owned Firearms.

11.1. Installation guidance governing use, possession, and control of Privately Owned Firearms (POFs) is in accordance with DoD policy, Air Force Instructions, MAJCOM guidance, and the 502 ABW/CC's risk tolerance, while remaining in compliance with federal, state, local and tribal laws. The 502 ABW/CC has taken the necessary and lawful measures to maintain good order and discipline and security. This includes the authority to deny access, detain or remove individuals who threaten the safety or orderly administration of an installation, and to control the possession, storage and transportation of POFs.

11.2. The only authorized storage areas on JBSA permitted for privately owned firearms and ammunition are military family housing (MFH) and the Security Forces Armories located on each respective JBSA location (Note: Army units with Arms rooms, are authorized to store POFs belonging to their assigned personnel).

11.3. Privately owned firearms stored in MFH will be stored/secured, unloaded, and in a manner that prevent access to the POF by juveniles and unauthorized persons. The only approved methods of storage are with a trigger lock, metal locking gun case or firebox, or in a tamper-proof display case. If a display case is used, the case must have break-proof or wire-mesh reinforced glass with a tamper-proof locking device. Ammunition may be stored in the same container as the firearm but will not be stored in the weapon. If a housing

resident is not able to comply with these standards, they must store their POF in the servicing SFS armory or Army unit Arms room.

11.4. POFs will not be maintained or stored at any time within JBSA billeting facilities such as (BOQ, VOQ, VAQ, TLF, or leased hotels on government property) or within any JBSA military barracks/dormitories.

11.5. POFs removed from MFH, SFS armory or Army Arms rooms will be immediately transported off the installation by the most direct route. Upon returning onto the JBSA property, the firearms will be unloaded and out of reach of vehicle occupants. The firearms will be returned to its authorized storage area immediately.

11.6. Commanders may determine when POFs must be stored in the SF armory or Army Arms room for the good order, discipline and safety reasons. Commanders may prohibit withdrawal of POFs and ammunition from SF armories or Army Arms rooms by persons under their command.

11.7. Transporting POFs within JBSA. **Note:** The below provisions do not apply to Federal, State, Local, and Tribal law enforcement officials on official duties or invited by a military authority.

11.7.1. Place weapons/firearms out of arms reach.

11.7.2. Keep firearms unloaded with ammunition separate from the weapon (example: store the ammunition in the glove compartment and the firearm in the trunk) out of immediate reach. Note: Firearm and ammunition may be stored in a pickup truck cabin provided that the firearm is unloaded, and the ammunition is kept separate.

11.8. Registration of POFs stored on JBSA locations <u>is mandatory.</u> POFs are never allowed to be stored in any other facility/building or vehicle on JBSA to include dormitories, billeting, offices, etc. Newly assigned personnel living in privatized housing have up to 30 days to register their POFs or other weapons.

11.8.1. The AF Form 1314 will be used to register up to five weapons/firearms per individual. Additional AF Form 1314 may be used as required to register additional firearms. Forms and registration information can be obtained from the 502 SFG Access Control Manager or at a Security Forces VCC.

11.8.2. Unit Commanders will direct the registration and storage of firearms at one of the authorized locations on the JBSA.

11.9. Reporting of POF and weapons misuse or violations. The discharge of any firearm on JBSA is prohibited, except during the performance of official duty, authorized/sanctioned shooting events on the installation such as firing ranges, SFS and AFOSI personnel performing official duties, and Airfield Management's use for Bird Wildlife Aircraft Strike Hazard (BASH) program.

11.9.1. All JBSA personnel are required to report weapons or firearms violations by individual's exhibiting behaviors or actions not consistent with responsible use or security or safety of firearms (including concerns of harm to self or others) to the appropriate command authority and installation Security Forces personnel.

11.10. Firearms and Weapons Education. Leaders at all levels will ensure unit personnel receives security awareness regarding mandates or restrictions of DoD, AF, MAJCOM and JBSA weapons and firearms instructions.

11.11. Reporting loss or theft of firearms. Reports are made immediately upon discovery to Security Forces Base Defense Operation Center.

12. Carry of POFs. The open or concealed carry of privately-owned weapons/firearms on JBSA owned, rented or leased property is strictly prohibited.

13. Prohibited Weapons and Firearms. The following are considered illegal unless specifically authorized by competent authority, and are not permitted on JBSA (a violation of this paragraph or any subparagraph may result in UCMJ disciplinary, criminal or administrative action):

13.1. Switchblade knives, knives three (3) inches or longer or knives with any automatic blade release (unless military duty issued).

13.2. Any incendiary/explosive weapon (e.g., grenades, flashbangs).

13.3. Fireworks, except as authorized by approved contractors during organized/sanctioned JBSA events.

13.4. Suppressors and or silencers. Any device designed, made or adapted to muffle the report of a firearm.

13.5. A short barrel rifle (SBR – a rifle with a barrel less than 16" and overall length less than 26"), short barrel shotgun (SBS – a shotgun with a barrel less than 18" and overall length less than 26"), any other weapon (AOW) or destructive device (DD).

13.6. Homemade mortars, aka "tennis ball launchers," "potato guns" or similar devices.

13.7. Machine Guns. Any weapon capable of full-automatic fire.

14. Installation Debarment. Directives issued by the 502 ABW/CC governing the entry/exit from JBSA are enforceable, in accordance with Section 21 of the Internal Security Act of 1950 (50 United States Code [USC] 797), against all persons, regardless if those persons are subject to the Uniformed Code of Military Justice (UCMJ). Military personnel who re-enter JBSA after receiving an order not to re-enter will be apprehended. Civilian violators will be detained/cited under (18 USC Section 1382 – Trespassing) and either escorted off the installation or turned over to proper civilian authority.

14.1. Authority. The 502 ABW/CC has the authority under DoD Instruction 5200.8, *Security of DoD Installations and Resources,* and the Internal Security Act to deny an individual access to JBSA with a debarment order or letter. This authority is not delegable. Debarments are issued to individuals involved or suspected of a criminal offense, when access onto the installation is inconsistent with national security, or when access to the installation adversely affects the health, safety, or morale of JBSA personnel.

14.2. The scope of Debarment. By direction of the 502 ABW/CC, individuals barred from one JBSA location are automatically barred from all JBSA locations unless otherwise specified in the debarment order or letter.

14.3. Delivery of Debarments. Debarments are delivered via a letter or memorandum. However, the 502 ABW/CC may issue oral debarment orders when offenses, actions, or information about an individual warrant immediate debarment or time constraints prevent completing a written order. All oral debarments must be followed by written order or letter within 24 hours or the next duty day.

14.4. Reasons for Debarment. Violations requiring debarment include but are not limited to:

14.4.1. Violations of force protection or integrated defense measures including but not limited to disorderly conduct, failure to obey an order or another proper directive, failure to enter the installation at or circumventing a designated access control point and attempting to enter under false pretenses.

14.4.2. Rape, sexual assault and other sexual misconduct.

14.4.3. Burglary.

14.4.4. Indecent exposure.

14.4.5. Violation of civil "no contact" or protective orders.

14.4.6. Possession of child pornography at any location under control of 502 ABW/CC.

14.4.7. Driving under the influence of alcohol or drugs.

14.4.8. Unlawful use, possession or actual/attempted distribution of a controlled substance.

14.4.9. Larceny/Theft of government or private property, to include shoplifting Army Air Force Exchange Service (AAFES) and Commissary merchandise.

14.4.10. Willful damage or destruction of government/private property.

14.4.11. All categories of assault.

14.4.12. Unlawfully carrying, transporting, or possessing a weapon or weapon accessory, whether concealed or unconcealed, without legal justification or commander approval.

14.4.13. Contributing to the delinquency of a minor.

14.5. Legal Considerations.

14.5.1. Active duty personnel may not be barred entirely from JBSA or any facility to which assigned, employed, or required to enter on official mission-related business. However in lieu of full debarment, they may be given limited or restricted access to specific employment-related areas or facilities.

14.5.2. Civilian employees include appropriated and non-appropriated employees and contractor employees may be barred by limiting access only to the place of work or areas of the installation where employment-related needs exist. However, they may be potentially barred entirely from JBSA or the facility to which they are assigned or employed.

14.5.3. Active duty and retired military, DoD civilians, and their family members may be entitled to have access to medical and dental facilities. Thus, specific provisions for limited access will be offered and explained in detail with the debarment letter or memorandum.

14.6. Installation Access Reinstatement. The 502 ABW/CC has access reinstatement authority, and such authority may not be delegated.

14.6.1. Individuals on the debarment roster may request reinstatement of access privileges to the 502 ABW/CC. The commander may deny or reinstate privileges.

14.6.2. If the reinstatement is approved, other agencies previously informed of the debarment action will be notified of the removal.

14.7. Debarment Appeals.

14.7.1. Debarment letters or orders will contain specific instructions regarding appeals. Individuals may appeal debarment action if:

14.7.1.1. Debarment was enacted based on mistaken identity.

14.7.1.2. Administrative errors occurred that directly led to the debarment determination.

14.7.1.3. Appeals will be submitted in writing to the 502 ABW/CC through the 502 FSG/JA and the respective SFS (502, 802, or 902) Reports and Administration Flight (S5R) within 30 days of debarment action and must include evidence that the debarment was enacted in error.

14.7.1.4. Commanders will endorse appeals originating from active duty members on behalf of themselves or family members.

14.8. Debarment Process.

14.8.1. The 502 SFG/CC in consultation with 502 FSG/JA and 502 ABW/CC will determine the debarment actions. Appropriately, the Civilian Personnel Office and appropriate Contracting Officer coordination are required.

14.8.2. The respective SFS will manage the debarment process. Provide all debarment supporting documentation per AFI 31-120, *Security Forces Systems, and Administration*.

14.8.2.1. Establishes procedures to deliver debarment memorandum or letter. Maintains official debarment files IAW RDS.

14.8.2.2. Maintains current debarment rosters and databases are updated with debarment actions.

15. Special Events.

15.1. Hosting a large function (six or more visitors) requires submission of a JBSANANTONIO Form 7, *Unescorted Access Request,* to VCC where the event is being conducted. The host or sponsor must e-mail an encrypted message within 10 days of the event, via a .mil e-mail or hand-carry a typed list.

15.2. Commands, organizations, or units assigned hosting special events such as air shows, open houses, concerts, and community celebrations. Depending on the special event, it may become unrealistic to properly identity proof and vet everyone in attendance. Therefore, compensatory measures to control circulation of un-vetted personnel and ensure the overall security of the special event, participants, and attendees compensatory measures must be taken, and submission of JBSANANTONIO Form 6, *Special Events Notification Worksheet*

to the 502 ABW/XP via email at **usaf.jbsa.502-abw.mbx.fsh-xp3-current-operations@mail.mil**, no less than 180 days prior to the event start date is required.

15.3. Security Forces supporting the special event will complete **Attachment 7** if required.

16. Credentials Confiscation. Credentials are government property. Security Forces may confiscate identification credentials, cards, and similar documents. When a credential holder employment is terminated, or credential is expired, fraudulently used or mutilated, or presented by an individual not entitled to use it.

16.1. Expired. Includes affiliation to employment, contract, or service separation, discharge, or termination.

16.2. Altered, Mutilated or Illegible.

16.3. Shoplifting.

17. News Media and Tours Access.

17.1. Media. Press and other media representatives may be granted access after coordination through the JBSA Public Affairs Office (PAO). PAO will provide media information to include the number of vehicles, personnel visiting, and destination.

17.1.1. News media representatives must have a PAO escort. After working hours, on weekends and holidays, coordinate entry authorization for media with the PAO. News media representatives will always be escorted while on JBSA locations.

17.2. Tours. Public Affairs must arrange escorted access onto the installation for tours. Tours arriving after hours will be denied access unless previously coordinated with 502 ABW/PA.

18. Disclaimer. Entry control policy and procedures are subject to change at any time by direction of the Installation Commander.

LAURA L. LENDERMAN, Brigadier General, USAF
Commander, 502d Air Base Wing

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 10-701, *Operations Security (OPSEC),* 8 June 2011 (AFI10-701_AFGM2018-01, 20 Jul 18)

AFI 10-1001, *Civil Aircraft Landing Permits*, 1 September 1995

AFPD 31-1, *Integrated Defense*, 28 October 2011

AFI 31-101, Security, *Integrated Defense (ID),* 5 July 2017 (AFI31-101_AFGM2018-03, 31 Dec18)

AFI 33-332, *The Air Force Privacy Act and Civil Liberties Program*, 12 January 2015

AFI 36-3026_IP Volume 1, *Identification Cards for Members of the Uniformed Services, Their Eligible Family Members, and Other Eligible Personnel*, 4 August 2017

AFTTP 3-31.1 *Entry Control*, 29 May 2007

DoDI 5200.08, *Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB),* Incorporating Interim Change 2, 8 April 2014

DoDD 5200.27, *Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense*, 7 January 1980

DoDD 5230.20, *Visits and Assignments of Foreign Nationals*, 22 June 2005

DoDD 5400.11, "DoD Privacy Program," 29 October 2014

DoD 5400.11-R, "Department of Defense Privacy Program," 8 May 2007

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

JBSA IDP, *Integrated Defense Plan,* 28 May 2018

FAR, *Federal Acquisition Regulation*

AFFAR, *Air Force Federal Acquisition Regulation*

OMB M-05-24, Office of Management and Budget Memorandum (M-05-24), *Implementation of Homeland Security Presidential Directive-12-Policy for a Common Identification Standard for Federal Employees and Contractors*, 5 August 2005

Section 552a of Title 5, United States Code (also known as "The Privacy Act of 1974")

JSFOI 31-113, *Installation Perimeter Access Control*, (Ch 1.) 13 June 2016

JSFOI 31-113A, *Visitor Control Center Operations*, 6 May 2016

JSFOI 31-120, *Security Forces Administration and Reports*, 22 September 2016

Prescribed Forms

JBSANANTONIO Form 6, *Joint Base San Antonio Special Event Notification Worksheet*

JBSANANTONIO Form 7, *Unescorted Access Request*

Adopted Forms

AF Form 1314, *Firearms Registration*

DD Form 2760, *Qualification to Possess Firearms*

Terms

Access Control—The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). A function or a system that restricts access to authorized persons only.

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 the physical proximity of the sponsor except for 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.

Escorting Authority—Escort authority allows an individual, with an authorized form of identification that certifies he/she has been successfully identity proofed and favorably vetted, to vouch for any vehicle occupants entering the installation or pedestrians if walking through a pedestrian gate, and escort them onto an installation without identity proofing, vetting or pass issuance.

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.

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

Firearms—Defined in Section 921 of Title 18, U.S.C. (The term "firearm" means (A) any weapon (including a starter gun) which will or is designed to or may readily be converted to expel a projectile by the action of an explosive; (B) the frame or receiver of any such weapon; (C) any firearm muffler or firearm silencer; or (D) any destructive device. Such term does not include an antique firearm.)

Fitness—The level of character and conduct determined necessary for the basis of access control decisions.

Foreign Nationals—A "foreign national" is any person who is not a U.S. citizen or a person who is not a naturalized citizen.

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 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.

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

Restricted Area—Any area to which entry is subject to special restrictions or control for security reasons or to safeguard property or material. This does not include those designated areas over which aircraft flight is restricted. Restricted areas may be of different types. The type depends on the nature and varying degree of importance, from a security standpoint, of the security interest or other matter contained therein (Controlled, Limited or Exclusive).

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.

Sponsoring Authority—Sponsorship allows approved individuals affiliated with DoD to take responsibility for verifying and authorizing an applicant's need for a locally produced identification credential to facilitate unescorted access to an installation.

State Issued Card—A 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 applicants 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.

Weapon—Generally something used to injure, defeat, or destroy and may cover many types of instruments, such as a blackjack, slingshot, billy, metal knuckles, dagger, knife, pistol, revolver, or any other firearm, razor with an unguarded blade, and any metal pipe or bar used or intended to be used in a club, among others.

Attachment 2

INSTALLATION ACCESS CONTROL POINTS AND VISITOR CENTER FACILITIES

A2.1. Access Control Points (ACP): All ACP hours, closing days and openings are subject to change based upon mission requirements as deemed by the Defense Force Commander (DFC), Security Forces Group Commander (502 SFG/CC), Executive Agent (EA), or Installation Commander (502 ABW/CC). JBSA will only operate the minimum number of ACPs required for the mission or operational requirements. Current gate hours are as follows:

A2.1.1. Primary ACP (24 hours/7 days):

A2.1.1.1. **Joint Base San Antonio Fort Sam Houston (JBSA-FSH).**

A2.1.1.1.1. Walters ACP.

A2.1.1.1.2. Schofield ACP.

A2.1.1.1.3. Harry Wurzbach East ACP.

A2.1.1.1.4. I-35 ACP.

A2.1.1.1.5. Camp Bullis ACP.

A2.1.1.1.6. Winans ACP.

A2.1.1.2. **Joint Base San Antonio Lackland (JBSA-LAK).**

A2.1.1.2.1. Valley High ACP.

A2.1.1.2.2. Luke East ACP.

A2.1.1.2.3. General McMullen ACP.

A2.1.1.2.4. Medina Annex ACP.

A2.1.1.3. **Joint Base San Antonio Randolph (JBSA-RND).**

A2.1.1.3.1. Lindsey ACP.

A2.1.2. Secondary ACP (variable hours and days) Use Gates:

A2.1.2.1. **Joint Base San Antonio Fort Sam Houston (JBSA-FSH).**

A2.1.2.1.1. BAMC Beach ACP: 0600-1800 hrs Monday - Friday. Closed Weekends and Holidays.

A2.1.2.1.2. Jadwin ACP (& Commercial Traffic ACP): 0600-1800 hrs Monday - Friday. Closed Sat/Sun. **Note.** Commercial traffic will either use Jadwin ACP or Walters Commercial Vehicle Search.

A2.1.2.1.3. New Braunfels ACP: 0600-2200 hrs Sunday-Saturday.

A2.1.2.1.4. Wilson ACP: 0600-1300 hrs Monday – Friday. Closed Weekends and Holidays.

A2.1.2.1.5. Harry Wurzbach West ACP: 0600-0900 hrs Monday - Friday. Closed Weekends and Holidays.

A2.1.2.1.6. Quad Pedestrian Gate: 0600-1800 hrs Monday – Friday (Pedestrian traffic only). Closed Sat/Sun.

A2.1.2.2. **Joint Base San Antonio Lackland (JBSA-LAK).**

A2.1.2.2.1. Luke West ACP (Gate 3): 0600-0900 hrs (inbound) & 1500-1800 hrs (outbound). Thursdays and Fridays 0600 – 1800. Closed Sat/Sun and Federal Holidays except for Thursday and Friday.

A2.1.2.2.2. Selfridge West ACP (Gate 4): 0600-0900 hrs (inbound) & 1500-1800 hrs (outbound). Thursdays and Fridays 0600 – 1800 hrs. Closed Sat/Sun and Federal Holidays except for Thursday and Friday.

A2.1.2.2.3. Selfridge East ACP (Gate 5): 0600-1800 hrs (Monday – Friday). Closed Sat/Sun and Federal Holidays.

A2.1.2.2.4. Security Hill ACP (Gate 9): 0600-1800 hrs (Monday – Friday). Closed Sat/Sun and Federal Holidays.

A2.1.2.2.5. Growden ACP (Gate 10): Mon-Fri: 0500-1800 hrs, Sat-Sun: 0500-1700 hrs. Closed Federal Holidays.

A2.1.2.2.6. Growden ACP (Search 10): Mon-Fri: 0500-1800 hrs, Sat-Sun: 0500-1700 hrs. Closed Federal Holidays.

A2.1.2.2.7. Medina ACP (Search 1): Mon-Fri: 0600-1800 hrs. Closed Sat-Sun.

A2.1.2.2.8. Tinker ACP (Search 13): Mon-Fri: 0600-1800 hrs. Closed Sat-Sun.

A2.1.2.3. **Joint Base San Antonio Randolph (JBSA-RND).**

A2.1.2.3.1. East ACP: 0600-0830 hrs (inbound) & 1500-1730 hrs (outbound).

A2.1.2.3.2. West ACP: 0600-1800 hrs. Closed Sat/Sun.

A2.1.2.3.3. South ACP: 0600 - 0830 hrs (inbound only) 0830-1800 hrs both in/outbound (Monday-Friday). Closed Sat/Sun.

A2.2. Visitor Control Centers (VCCs). The VCC is the primary Security Forces facility for the registration and issuance of installation access credentials. The VCCs, phone numbers, contact information and their hours of operation are listed below:

A2.2.1. **Joint Base San Antonio Fort Sam Houston (JBSA-FSH).** The organizational email address for all JBSA-FSH VCCs is **usaf.jbsa.502-abw.list.502-sfs-fsh-visitor-control-center-owner@mail.mil**.

A2.2.1.1. Walters VCC: Mon-Sun: 0600-1800 hrs. Closed Federal Holidays. Phone number: (210) 221-2650.

A2.2.1.2. I-35 VCC: 24/7. Phone number: (210) 539-9825.

A2.2.2. **Joint Base San Antonio Lackland (JBSA-LAK).** The organizational email address for all JBSA-LAK VCCs is **lackland.vrc@us.af.mil**.

A2.2.2.1. Luke East VCC: 24 hours, Sun-Sat operations. Phone number: (210) 671-6174.

A2.2.2.2. Valley High Pass and Registration: Mon-Fri: 0730-1630 hrs. Closed Federal Holidays. Phone number: (210) 671-1457.

A2.2.2.3. Building 171 VCC: Mon-Fri: 0600-1600. Closed Federal Holidays. Phone number: (210) 395-0043.

A2.2.3. **Joint Base San Antonio Randolph (JBSA-RND).** The organizational email address for the JBSA-RND VCC is **902sfs.vrc@us.af.mil**.

A2.2.3.1. Lindsey (Main ACP) VCC: Mon-Fri 0700-1630 hrs. Closed weekends, Federal Holidays and AETC Family days. Phone number: (210) 652-3939.

Attachment 3

IDENTITY PROOFING CREDENTIALS

A3.1. A proofing credential is a physical document issued by the Federal, State, or local government that attests to one's identity. One form of the following documents will be accepted as proof of identity. The document must be a picture ID and all documents must be valid.

A3.1.1. United States Passport. The U.S. Department of State issues the U.S. Passport to U.S. citizens and nationals.

A3.1.2. Form I-551, *Permanent Resident Card/Alien Registration Receipt Card*. The Permanent Resident Card shows the Department of Homeland Security (DHS) seal and contains a detailed hologram on the front of the card. Each card is personalized with an etching showing the bearer's photo, name, fingerprint, date of birth, alien registration number and card number.

A3.1.3. Foreign passport with a temporary (I-551) stamp or temporary (I-551) printed notation on a machine readable immigrant visa. U.S. Customs and Immigration Services (USCIS) uses either a I-551 stamp or a temporary I-551 printed notation on a machine-readable immigrant visa (MRIV) to denote temporary evidence of lawful permanent residency. **Note:** Another identity proofing document must be requested if the stamp or MRIV expires, or one year after the issuance date if the stamp or statement does not include an expiration date.

A3.1.4. North Atlantic Treaty Organization (NATO) military members traveling on NATO orders will not be required to present any of the forms above. NATO military members traveling on official NATO orders will present their NATO travel orders in order to determine need for access and must be in possession of a Host Nation (HN) government identification card in order to be considered identity proofed. This does not waive the requirement for vetting.

A3.1.5. An employment authorization document that contains a photograph (Form I-766, *Employment Authorization Document*). USCIS issues the Employment Authorization Document to aliens granted temporary employment authorization in the United States. The card contains the bearer's photograph, fingerprint, card number, Alien number, birth date, signature, holographic film and the DHS seal. The expiration date is located at the bottom of the card.

A3.1.6. U.S. Coast Guard Merchant Mariner Legacy Cards. New credential will look and feel exactly like a passport. The cover will be embossed with holographic images, invisible until exposed to Ultraviolet (UV) light.

A3.1.7. Current/Valid Issued Driver's License or Identification card issued by a state or outlying possession of the United States provided it contains a photograph and biographic information such as name, date of birth, gender, height, weight, eye color, and address.

A3.1.8. Current/Valid issued Federal, State, or local Government issued identification card provided it contains a photograph and biographic information such as name, date of birth, gender, height, weight, eye color, and address.

A3.1.9. Transportation Worker Identification Card (TWIC).

Attachment 4

FITNESS DETERMINATI ON MATRIX

A4.1. The following matrix identifies categories that will result in denial of installation access.

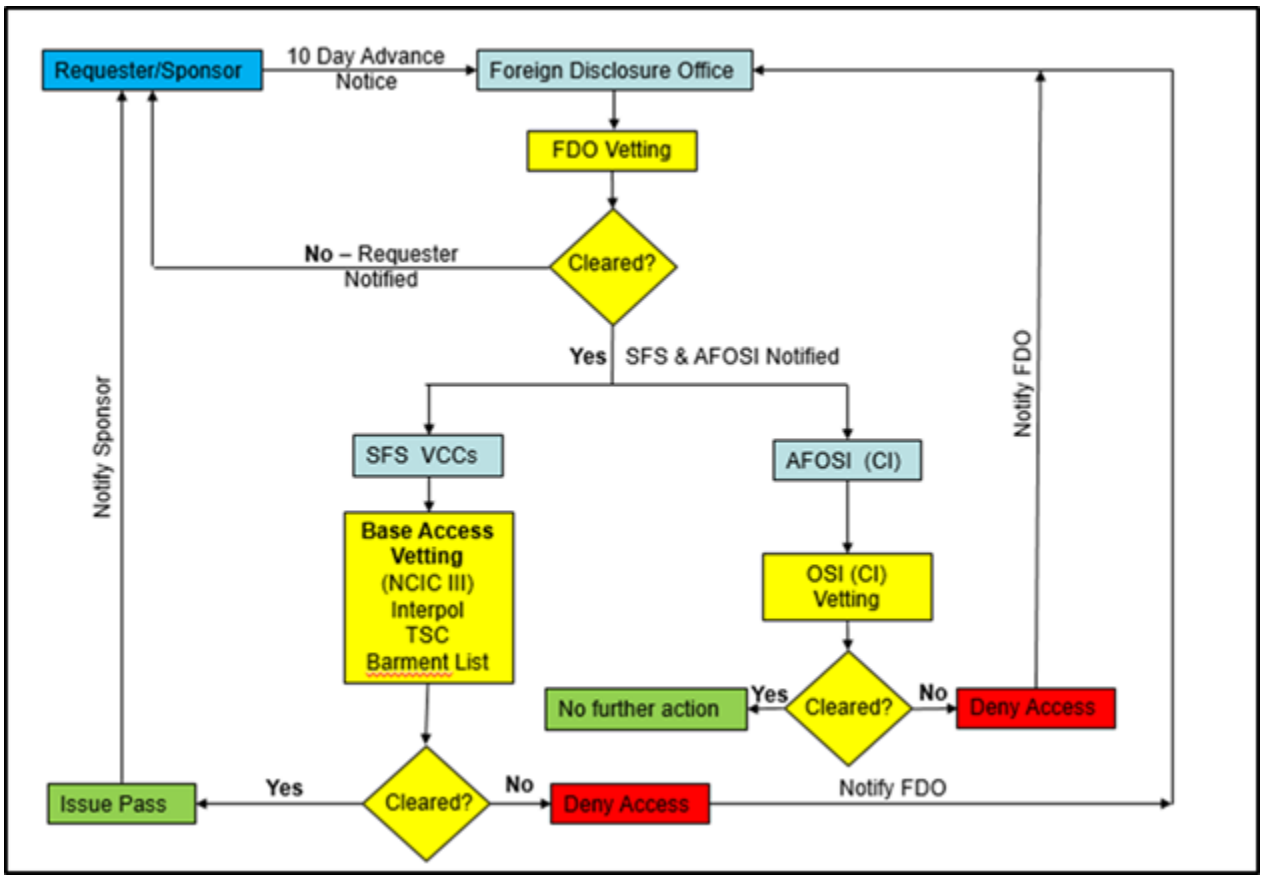
Table A4.1. Negative Fitness Determination Matrix.

Offense Type Description	***Date (In Years) Since Criminal Activity***	***Offense Type Description***	***Date (In Years) Since Criminal Activity***
Active Wants/Warrants	Until cleared	Housebreaking	3
Aiding Prisoner to Escape	Indefinite	Indecent Act With Child to include child molestation	Indefinite
Aiding the Enemy	Indefinite	Indecent Exposure	2
Arson	10	Kidnapping/Abduction (of an Adult)	Indefinite
Assault and Battery	3	Kidnapping: Child (Not Parent)	Indefinite
Assault Offenses (Aggravated Assault)	10	Larceny/Theft Offenses (Less than $500)	1
Assault: Milt/Civ Law Enforcer	10	Manslaughter	10
Assault: Simple	1	Motor Vehicle Theft	3
Bomb Threat	10	Murder	Indefinite
Burglary	5	Probation/Parole	Until sentence served
Child Pornography	Indefinite	Prostitution Offenses (Assisting or Promoting)	2
Communicating a Threat	1	Rape	Indefinite
Counterfeiting/Forgery	5	Robbery	10
Drugs: Manufacture, Possess, Sell or Distribute	10	Robbery, Armed	30
Embezzlement	5	Sex Offenses, Forcible	Indefinite
Espionage	Indefinite	Smuggling	5
Firearm, Felony Offenses	3	Sodomy of a Child or by Force	Indefinite
Gang Affiliation	Indefinite	Spying	Indefinite
Homicide	Indefinite	Trafficking in Persons	Indefinite

Attachment 5

FOREIGN VISITOR PROCESS

Figure A5.1. Foreign Visitor Pass Process Chart.



Attachment 6

KEY CONTACT NUMBERS

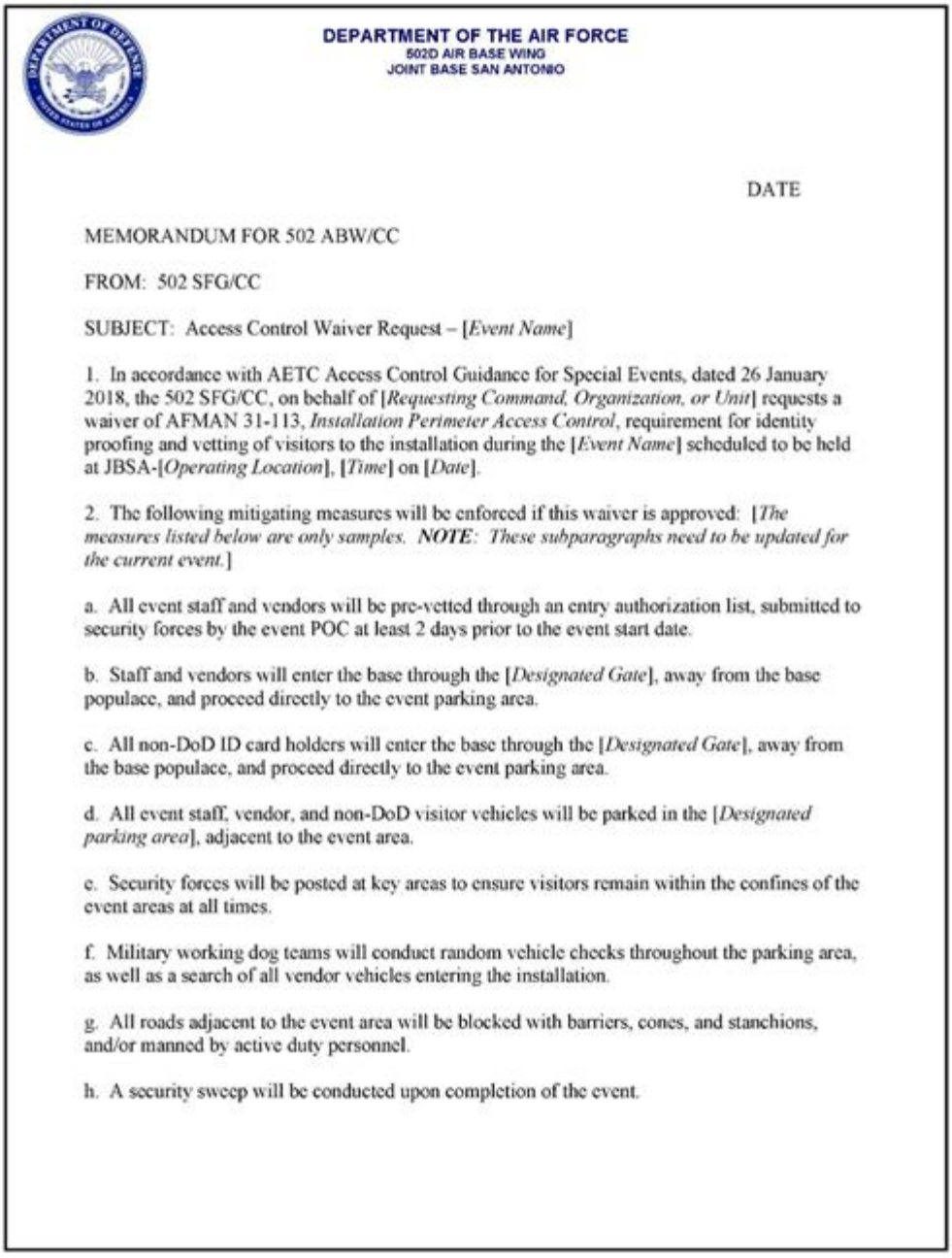
Table A6.1. Key Contact Number Listing.

Office	Title	Phone Number
502 SFG	Access Control Manager	(210) 652-5751
502 SFS (Fort Sam Houston)	Walters VCC	(210) 221-2650
502 SFS (SAMMC)	I-35 VCC	(210) 539-9825
802 SFS (Lackland)	Luke East VCC	(210) 671-6174
802 SFS (Lackland)	Valley High Pass and ID	(210) 671-1457
802 SFS (Lackland)	Building 171 VCC	(210) 395-0043
902 SFS (Randolph)	Lindsey (Main Gate) VCC	(210) 652-3939
502 SFS (Fort Sam Houston)	Base Defense Operations Center	(210) 221-9331
802 SFS (Lackland)	Base Defense Operations Center	(210) 671-2018
902 SFS (Randolph)	Base Defense Operations Center	(210) 652-5700
502 SFG	Foreign Disclosure Office	(210) 652-5762

Attachment 7

ACCESS CONTROL WAIVER REQUEST MEMORANDUM

Figure A7.1. Access Control Waiver Request Memorandum Example.



DEPARTMENT OF THE AIR FORCE
502D AIR BASE WING
JOINT BASE SAN ANTONIO

DATE

MEMORANDUM FOR 502 ABW/CC

FROM: 502 SFG/CC

SUBJECT: Access Control Waiver Request – [*Event Name*]

1. In accordance with AETC Access Control Guidance for Special Events, dated 26 January 2018, the 502 SFG/CC, on behalf of [*Requesting Command, Organization, or Unit*] requests a waiver of AFMAN 31-113, *Installation Perimeter Access Control*, requirement for identity proofing and vetting of visitors to the installation during the [*Event Name*] scheduled to be held at JBSA-[*Operating Location*], [*Time*] on [*Date*].

2. The following mitigating measures will be enforced if this waiver is approved: [*The measures listed below are only samples.* ***NOTE****: These subparagraphs need to be updated for the current event.*]

a. All event staff and vendors will be pre-vetted through an entry authorization list, submitted to security forces by the event POC at least 2 days prior to the event start date.

b. Staff and vendors will enter the base through the [*Designated Gate*], away from the base populace, and proceed directly to the event parking area.

c. All non-DoD ID card holders will enter the base through the [*Designated Gate*], away from the base populace, and proceed directly to the event parking area.

d. All event staff, vendor, and non-DoD visitor vehicles will be parked in the [*Designated parking area*], adjacent to the event area.

e. Security forces will be posted at key areas to ensure visitors remain within the confines of the event areas at all times.

f. Military working dog teams will conduct random vehicle checks throughout the parking area, as well as a search of all vendor vehicles entering the installation.

g. All roads adjacent to the event area will be blocked with barriers, cones, and stanchions, and/or manned by active duty personnel.

h. A security sweep will be conducted upon completion of the event.

3. The Threat Working Group has reviewed the event details and concurs with the proposed mitigation measures. There are currently no credible reports of threats toward JBSA or this event.

4. My action officer for this waiver request is [*Name*], [*Unit*], [*Phone*] or [*e-mail address*].

JEFFREY F. CARTER, Colonel, USAF
Commander

Attachment:
Special Event Supporting Documents [*diagrams, maps, etc. to support waiver request*]

1st Ind, 502 ABW/CC DATE

MEMORANDUM FOR 502 SFG/CC

Approve/Disapprove.

LAURA L. LENDERMAN, Brigadier General, USAF
Commander