

**BY ORDER OF THE  
SECRETARY OF THE AIR FORCE**

**AIR FORCE INSTRUCTION 31-120**

**1 APRIL 2015**



**Security**

**SECURITY FORCES SYSTEMS AND  
ADMINISTRATION**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available for downloading or ordering on the e-Publishing website at <http://www.e-publishing.af.mil/>

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: AFSFC/SFOP

Certified by: AF/A7S  
(Col Richard McComb)

Pages: 65

Supersedes: AFI 31-203, 29 July 2009;  
AFMAN 31-201V7,  
28 August 2009

---

This instruction implements Air Force Policy Directive (AFPD) AFPD 31-1, *Integrated Defense*. It provides guidance on general Security Forces systems, law enforcement operations and the Security Forces Administration and Reports Branch (S5R). Security Forces Management Information System (SFMS) and use of the Defense Biometric Identification System (DBIDS) is mandatory. **EXCEPTION:** The Pass and Registration module in SFMS is only mandatory for use if the installation does not have DBIDS. In addition, those installations which are Joint Based will follow lead agency policy. Compliance with this instruction is mandatory and applies to Department of the Air Force military, civilian, Reserve, Air National Guard, personnel from other US military branches assigned or attached to Air Force units, contract Security Forces, government-owned, contractor-operated (GOCO) and contractor-owned, contractor-operated (COCO) facilities. The terms "must," "shall" and "will" denote mandatory actions in this instruction. It is not necessary to send implementing publications to the higher headquarters functional officer of Primary Responsibility (OPR) for review and coordination before publishing. Refer recommended changes and conflicts between this and other publications to Headquarters Air Force Security Forces Center (HQ AFSFC) HQ AFSFC/SFOP, 1517 Billy Mitchell Blvd Bldg. 954, Joint Base San Antonio-Lackland, Texas, 78236, using Air Force AF Form 847, *Recommendation for Change of Publication*, through appropriate MAJCOM functional chain of command. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN)33-363, *Management of Records*, and are disposed of IAW the Air Force Records Disposition

Schedule (RDS) located in the Air Force Records Information Management System (AFRIMS). This AFMAN implements multiple requirements external to the Air Force; requests for waivers for those specific items must be processed through command channels to the publication OPR for consideration. Military members who fail to adhere to certain provisions of this instruction, specifically, paragraphs 1.6. may face enhanced punishment under Article 92(1), UCMJ. Article 92(1) of the UCMJ does not apply to the members of the ANG while in Title 32 status, but, they may be subject to an equivalent article under a state military justice code. Failure to observe the prohibitions and mandatory provisions in paragraphs 1.6 of this publication by military members is a violation of Article 92 of the UCMJ and applicable federal and state laws. Failure by civilian and contract works subject them to applicable federal and state laws.

This Publication requires the collection and or maintenance of information protected by the Privacy Act (PA) of 1974, IAW System of Record Notice (F031 AF SP B applies and is available at <http://dpclo.defense.gov/Privacy/SORNs.aspx> The authorities to collect and/or maintain the records in this publication are 10 United States Code (U.S.C.) 8013 Secretary of the Air Force: powers and duties; delegation by the PA Systems Notice(s) is available at: <http://www.defenselink.mil/privacy/notices/usaf>.

<b>Chapter 1—SECURITY FORCES MANAGEMENT INFORMATION SYSTEM</b>	<b>6</b>
1.1. Background. ....	6
1.2. Responsibilities. ....	6
1.3. Defense Incident-Based Reporting System (DIBRS). ....	9
1.4. National Incident-Based Reporting System (NIBRS). ....	11
1.5. General Administrative Information. ....	11
1.6. Privacy Information. ....	12
1.7. SFMIS Capabilities. ....	13
1.8. On-Line Manual. ....	14
1.9. SFMIS Training. ....	14
1.10. Erroneous Incident Report Entries (EIRE). ....	14
1.11. Requests for SFMIS Information and Releasing SF Information to the Public. ....	15
<b>Chapter 2—DEFENSE BIOMETRICS IDENTIFICATION SYSTEM (DBIDS)</b>	<b>19</b>
2.1. Background. ....	19
2.2. Responsibilities. ....	20
2.3. Roles. ....	21
2.4. System Integration. ....	23
2.5. System Operation. ....	23

<b>Chapter 3—NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS)/NATIONAL CRIME INFORMATION CENTER (NCIC) AND ADDITIONAL SYSTEMS</b>	<b>25</b>
3.1. Program Definition. ....	25
3.2. Program Responsibilities. ....	25
3.3. Providing System Protection. ....	26
3.4. Criminal History Data. ....	26
Table 3.1. Handling Code 1. ....	27
Table 3.2. Handling Code 2. ....	28
Table 3.3. Handling Code 3. ....	29
3.5. Validation System and Records Maintenance. ....	30
3.6. Agencies Receiving NLETS/NCIC Service. ....	30
3.7. Additional SF Systems. ....	30
<b>Chapter 4—SECURITY FORCES FORMS</b>	<b>32</b>
4.1. AF Form 52, Evidence Tag. ....	32
4.2. AF Form 53, Security Forces Desk Blotter. ....	32
4.3. AF Form 75, Visitor/Vehicle Pass. ....	32
4.4. AF Form 1109, Visitor Register Log. ....	32
4.5. AF Form 1168, Statement of Suspect/Witness/Complainant. ....	32
4.6. AF Form 1176, Authority to Search and Seize. ....	32
4.7. AF Form 1199 Series of Restricted Area Badges. ....	33
4.8. AF Form 1313, Driver Record. ....	33
4.9. AF Form 1315, Accident Report. ....	33
4.10. AF Form 1361, Pick-Up/Restriction Order. ....	33
4.11. AF Form 1364, Consent for Search and Seizure. ....	33
4.12. AF Form 2586, Unescorted Entry Authorization Certificate. ....	33
4.13. AF Form 3226, Authority to Apprehend in Private Dwelling. ....	34
4.14. AF Form 3545 and AF Form 3545(A), Incident Report. ....	34
4.15. AF Form 3907, Security Forces Field Interview Data. ....	34
4.16. AF Form 4443, Law Enforcement and Physical Security Activities Report (LEPSAR). ....	34
4.17. DD Form 460, Provisional Pass. ....	34
4.18. DD Form 1408, Armed Forces Traffic Ticket. ....	35
4.19. DD Form 1920, Alcohol Influence Report. ....	35

4.20. DD Form 2701, Initial Information for Victims and Witnesses of Crime. .... 35

4.21. DD Form 2708, Receipt for Inmate or Detained Person. .... 36

4.22. United States District Court Violation Notice (USDCVN). .... 36

4.23. Federal Document-249 (FD-249)/Criminal Fingerprint Card. .... 37

4.24. R-84/Final Disposition Report. .... 37

4.25. US Army Criminal Investigation Laboratory (USACIL) DNA Database  
Collection Card. .... 37

**Chapter 5—SECURITY FORCES ADMINISTRATION AND REPORTS 38**

5.1. Security Forces Processing DD Form 1408, Armed Forces Traffic Ticket. .... 38

5.2. Security Forces Processing DD Form 1408, Armed Forces Traffic Ticket,  
rebuttals. .... 38

5.3. United States District Court Violation Notice. .... 39

5.4. Processing Incident Reports. .... 40

5.5. Forwarding of Driving/Criminal Records/Suspension, Revocation and  
Debarment. .... 41

5.6. Preparation of DUI/DWI, No Proof of Insurance or Revocation/Suspension of  
Base Driving Privileges Packages. .... 42

5.7. Notifying State Licensing Offices. .... 43

5.8. Debarment Authority. .... 43

5.9. Preparation of Revocation of Exchange/Commissary Privileges Packages. .... 43

5.10. Certified Mail Procedures. .... 44

5.11. Preparing Packages for Filing. .... 44

5.12. Requests for Information. .... 44

5.13. Conducting Local Records Checks. .... 45

5.14. Tracking Reports and Statistics. .... 45

5.15. Management and Disposition of Security Forces Files. .... 45

5.16. Disposition of Files from Active to Inactive and Staging. .... 45

5.17. Disposition of Debarment, AAFES & Driving Revocation Packages. .... 45

5.18. Sex Offenders. .... 46

**Chapter 6—LAW ENFORCEMENT INFORMATION EXCHANGE (LIX) AND  
DEPARTMENT OF DEFENSE LAW ENFORCEMENT DEFENSE DATA  
EXCHANGE (D-DEX) 47**

6.1. History. .... 47

6.2. Partner Systems. .... 47

6.3.	Access to Information Sharing Systems. ....	47
6.4.	Training and Certifications. ....	48
6.5.	Expectation of Use. ....	48
6.6.	Validation. ....	48
6.7.	Justification. ....	49
6.8.	Background Investigations. ....	49
6.9.	Reporting Results. ....	49
6.10.	Printing. ....	50
6.11.	Use of Photographs. ....	50
6.12.	Sanctions. ....	50
<b>Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>		<b>51</b>
<b>Attachment 2—SAMPLE MEMO</b>		<b>59</b>
<b>Attachment 3—TELEPHONE NUMBERS/ADDRESSES FOR STATE AGENCIES NOTE</b>		<b>60</b>
<b>Attachment 4—SAMPLE FORMAT FOR A DEBARMENT LETTER</b>		<b>64</b>

## Chapter 1

### SECURITY FORCES MANAGEMENT INFORMATION SYSTEM

#### 1.1. Background.

1.1.1. The Security Forces Management Information System (SFMIS) was developed to meet the Congressionally-mandated Defense Incident-Based Reporting System (DIBRS) requirements and improve Air Force Security Forces day-to-day operations. It also provides statistical data for various users and has grown to meet many other needs.

1.1.2. SFMIS complies with DIBRS reporting criteria and provides the means to monitor and tracks crime and integrate defense trends for analysis of criminal and threat statistical data for intel fusion. SFMIS is useful for analysis of Law and Order statistics and threat fusion. Future capabilities will be added to SFMIS through the HQ Air Force Security Forces Center (AFSFC) and Major Command (MAJCOM) Functional Review Board (FRB).

1.1.3. Access to SFMIS by any personnel should be carefully scrutinized to ensure integrity of the system and protection of For Official Use Only (FOUO) and Privacy Act information. (T-2)

1.1.4. SFMIS users must know and ensure they meet Privacy Act of 1974 requirements, and report data only to those who have a valid need to know. (T-2)

1.1.5. Criminal Activity Reporting. SFMIS fully complies with DIBRS reporting requirements Department of Defense Directive (DoDD) 7730.47, *Defense Incident-Based Reporting System (DIBRS)*, Department of Defense (DoD) 7730.47-M Volume 1, *Manual for Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements*, and DoD 7730.47-M Vol 2, *Manual for Defense Incident-Based Reporting System (DIBRS): Supporting Codes*.

#### 1.2. Responsibilities.

1.2.1. Headquarters Air Force (HAF/A4I): Serves as the Designated Accrediting Authority (DAA) for SFMIS.

1.2.2. HQ AFSFC:

1.2.2.1. Establishes policy and procedures for SFMIS.

1.2.2.2. Is the Air Force Office of Primary Responsibility (OPR) for SFMIS implementation, programming and System Administration.

1.2.2.3. Is the functional lead for developing SFMIS capabilities. Will develop standardized AF self-inspection checklist for AFI compliance and load into Management Internal Control Toolset (MICT)

1.2.2.4. Develops SFMIS and other Automated Information System requirements.

1.2.2.5. Ensures compliance with DoDI 7730.47 and establishes policies and procedures to implement the DIBRS. Reports DIBRS data once a month, or as necessary, to the Defense Manpower Data Center (DMDC).

1.2.2.6. Periodically reviews the system's use to ensure compliance by all MAJCOMs and their respective units.

1.2.2.7. Grants access when notified in writing by a MAJCOM A7S Director of the appointment of a Functional System Administrator (FSA) at a MAJCOM.

1.2.2.8. Directs corrective action on SFMIS errors.

1.2.2.9. Will hold monthly teleconferences with MAJCOMs to discuss current and future SFMIS requirements.

1.2.2.10. Participates in FRB meetings. The FRB consists of functional subject matter experts and meets to discuss SFMIS needs.

1.2.2.11. Participates in the Configuration Control Board (CCB).

1.2.2.12. Is responsible to design, acquire, install, integrate and support the information systems necessary to provide the Air Force with the right combat support information.

1.2.2.13. Will develop an Operational Requirements Document that will serve as the Performance Work Statement (PWS) for SFMIS projects.

1.2.2.14. May use contractors as necessary to meet Security Forces requirements.

1.2.2.15. Is responsible for appointing an Information Assurance Manager (IAM) for SFMIS IAW DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*. The IAM will be qualified IAW DoDD 8570.1, *Information Assurance (IA) Training, Certification and Workforce Management*.

### 1.2.3. MAJCOM A7S:

1.2.3.1. Will appoint a primary and alternate FSA to grant permissions and access for their units.

1.2.3.2. Should send a representative(s) to the FRB meetings. If unable to attend in person, MAJCOMs are encouraged to attend via teleconference.

### 1.2.4. MAJCOM FSA:

1.2.4.1. Must monitor units to ensure that reports of commander action on incident reports and traffic tickets are forwarded to DIBRS in a timely manner (commander's action completes the report for the DIBRS database).

1.2.4.2. Will not approve use of other automated programs as substitutes for existing SFMIS capability. **EXCEPTION:** Systems procured by AF/A7S to enhance or replace SFMIS capability is authorized, i.e., Defense Biometric Identification System (DBIDS) and approved commercial systems used to create Restricted Area Badge may continue to be utilized. Also, NGB/A7S approved secured commercial systems used to create Restricted Area Badges may continue to be utilized within ANG. Refer to AFI 31-101, *Integrated Defense*, for more information. (T-0)

1.2.4.3. Will grant specific access and roles when notified in writing by the Defense Force Commander (DFC) of the appointment of an FSA at an installation.

1.2.4.4. Must periodically check the use of SFMIS by units to ensure the system is being used as required.

1.2.4.5. Create and upload documents for units that do not have access to SFMIS, i.e., incident reports, citations, etc.; also update Commander's After-Action dispositions and maintain the record(s) as required per the records dispositions schedule.

1.2.5. Installation Commanders:

1.2.5.1. Must ensure all DIBRS-specified incidents and reports of command action are reported via SFMIS. (T-0)

1.2.5.2. Must ensure command action on incident reports and traffic tickets are reported via SFMIS and updated appropriately in the system. (T-0)

1.2.6. Defense Force Commander (DFC):

1.2.6.1. Will appoint primary and alternate FSAs, via appointment letter. (T-1)

1.2.6.2. Will establish internal controls to allow management to view each DIBRS-reportable incident. (T-2)

1.2.6.3. Will ensure all DIBRS-reportable incidents are entered and reported through SFMIS. (T-0)

1.2.6.4. Will ensure original reports of investigations (ROIs), AF Forms 3545A, *Incident Reports*, and United States District Court Violation Notice (USDCVN) are provided to Air Force Office of Special Investigations (AFOSI) for Defense Clearance and Investigations Index (DCII) reporting. (T-1)

1.2.6.5. Will coordinate with all base functions that may require informational or "live" access to SFMIS information. (T-2)

1.2.7. Reports & Analysis (S5R) and Security Forces Investigations (S2I):

1.2.7.1. S5R will perform a computer run of the previous month's Criminal Summary Report NLT the 5th duty day of each month and give the report to Security Forces Investigations (S2I). If the case is turned over to another agency, SFMIS will be marked in the appropriate blocks and agency information regarding who took over the case will be explained in the Narrative section. (T-3)

1.2.7.1.1. Process information for units that do not have access to SFMIS and maintain the record(s). (T-3)

1.2.7.2. S2I will compare the report with the local AFOSI detachment point of contact to ensure all DCII information is reported. (T-1)

1.2.8. Functional System Administrator (FSA):

1.2.8.1. Will act as the local grantors of roles and level of access for personnel requiring access to SFMIS. (T-3)

1.2.8.2. Will delete SFMIS account(s) within 48 hours of Permanent Change of Station (PCS), retirement or separation. This will be added to each unit's out-processing checklist. If an individual is under investigation, their access to SFMIS will be suspended until the impending investigation is cleared. (T-2)

1.2.9. Local Security Forces Units: Will verify with local law enforcement agencies at the beginning of each shift for any civil incarceration of military personnel on active duty to ensure DIBRS-related information is submitted via SFMIS. (T-1)

1.2.10. SFMIS Users:

1.2.10.1. All SFMIS users are required to read their responsibilities of safeguarding SFMIS information and sign acknowledging these responsibilities. All units will keep on file the acknowledgement of responsibilities for personnel within their unit. A copy of the responsibilities of safeguarding information along with the acknowledgement of responsibilities can be found on the Security Forces SMARTNet (<https://afsfmil.lackland.af.mil/>)

1.2.11. Air Force Corrections:

1.2.11.1. Local SF corrections officials will enter inmate information into the SFMIS Confinement Module, as well as report the case outcome to S5R. This requirement applies to all SF units regardless of whether they have an organic confinement facility or not. The only exception is Air Force inmates confined in civilian facilities on civilian charge(s). (T-1)

1.2.11.2. The SF unit Confinement Officer or point of contact will ensure an entry is completed on every member sentenced to confinement by a court-martial. **NOTE:** Personnel referred to USAF SF Level I confinement facilities must have the crime resulting in their confinement reported to DIBRS via SFMIS or AFOSI channels. (T-1)

1.2.11.3. Non SF investigations/cases for inmates cannot be entered into the Confinement Module (i.e., AFOSI cases). A new incident report will need to be accomplished to be able to enter non SF investigations into SFMIS. (T-2)

1.2.11.4. Once the incident report is created, the person initiating the report clicks the "OSI Reference" button in the incident report segment and will add basic information regarding the case and will note "Refer to AFOSI" in the narrative section. (T-2)

### **1.3. Defense Incident-Based Reporting System (DIBRS).**

1.3.1. DIBRS is primarily a reporting system covering all active duty, reserve, federal employees, family members and guard military personnel. DIBRS is DoD's centralized reporting system to the Federal Bureau of Investigation's National Incident-Based Reporting System (NIBRS). It implements reporting requirements of:

1.3.1.1. Section 534 of Title 28, United States Code (also known as "The Uniform Federal Crime Reporting Act of 1988") (Reference (c)).

1.3.1.2. The victim and witness assistance notifications of Sections 10601 through 10608 of Title 42 (also known as "The Victims' Rights and Restitution Act of 1990") (Reference (d)).

1.3.1.3. Section 922 of Title 18, United States Code (also known as "The Brady Handgun Violence Prevention Act and The Lautenberg Amendment to the Gun Control Act") (Reference (e)).

1.3.1.4. Sections 16901 through 16928 of Title 42, United States Code (also known as “The Jacob Wetterling, Megan Nicole Kanka and Pam Lychner Sex Offender Registration and Notification Program”) (Reference (f)).

1.3.1.5. Public Law 107-188 (Reference (g)).

1.3.1.6. The establishment of a central Air Force database on domestic violence incidents.

1.3.2. Active, Reserve and Air National Guard Security Forces units will comply with the reporting requirements mandated by Congress and outlined in DoDD 7730.47, *Defense Incident-Based Reporting System (DIBRS)*, and DoD 7730.47-M Volume 1, *Manual for Defense Incident-Based Reporting System*. For definitions of reportable incidents, refer to DoD 7730.47-M, Volume 2, *Manual for Defense Incident-Based Reporting System*. (T-0)

1.3.3. DIBRS reporting is triggered when Security Forces respond to a credible report of a criminal incident. Typically, any Security Forces response which requires more than an AF Form 1168, *Statement of Suspect, Witness or Victim*, requires a report to ensure DIBRS reporting. Security Forces shall collect information necessary to fulfill reporting responsibilities, including the data required by NIBRS.

1.3.3.1. If a military member commits a crime outside the jurisdiction of the federal government (e.g., civilian police agency), DIBRS reporting is still required. Civil agencies will typically complete NIBRS reporting, but not DIBRS. In these instances, Security Forces will complete the DIBRS requirement. (T-0)

1.3.3.2. In the event an agency (e.g., Defense Criminal Investigative Organizations, Federal Bureau of Investigations (FBI), or AFOSI) with jurisdiction takes responsibility for a criminal incident, DIBRS reporting passes to them. Security Forces must not report information in these situations to prevent double reporting in DIBRS. (T-0)

1.3.4. DIBRS submissions must be completed by the 15th day of each month. DIBRS submissions pending final action, to include the report of commander’s action, must be tracked until final disposition. (T-0)

1.3.4.1. Air National Guard (ANG) and Air Force Reserve Command (AFRC) units will run their reports once a month. This can be accomplished by the DFC appointed SFMIS monitor or the alternate. (T-0)

1.3.4.2. ANG and AFRC Security Forces units which are co-located on active duty Air Force bases will not run the Criminal Summary Report. These entities will forward the DIBRS-reportable information to the active duty host Security Forces unit, who will perform the computer run of the previous month’s Criminal Summary Report. ANG Security Forces units that are co-located on sister service installations will forward DIBRS reportable information to the host Law and Order/Provost Marshal’s Office. (T-2)

1.3.5. Units must identify and correct DIBRS errors. DIBRS errors occur when information placed into SFMIS is incorrect. SFMIS will give a visual warning to the user indicating an error on the page where data is entered. (T-2)

1.3.6. The AF Form 3545A or Report of Investigation (ROI) records the data reportable to the DMDC for DIBRS submission. Incidents not covered by DIBRS will be documented and

reported under Uniform Code of Military Justice guidelines. **NOTE:** Reports of Survey (ROS) are often related to the theft, loss or damage of government property, which are also usually DIBRS reportable. An ROS can be added to an AF Form 3545 as an attachment. The purpose of an ROS is to determine if the person is accountable for the item and does not establish criminal activity. AF Form 3545A is a SFMIS generated incident report. An AF Form 3545 is used at locations where SFMIS is not available and can be downloaded from AF e-Publishing. Once completed, the unit then forwards the report to the subject's home station for upload in SFMIS. (T-1)

1.3.6.1. The SFMIS-generated Incident Report Summary (AF Form 3545A) or an original AF Form 3545, with original signature or digital signature on the Commander's Action page, is approved for use as the final file copy.

1.3.6.2. The disposition of a commander's action is mandatory for DIBRS reporting. On a yearly basis, DMDC provides DoD with DIBRS data on criminal statistics. One of the major areas reviewed are the commander's action reports. A list of the commanders' actions taken or not taken is required. To ensure Air Force compliance, SF unit FSAs will conduct a monthly review of all pending cases and attempt to finalize them. An incident is finalized when it is adjudicated and has the commander's signature. (T-0)

#### **1.4. National Incident-Based Reporting System (NIBRS).**

1.4.1. NIBRS is the overall reporting system DIBRS feeds into. NIBRS originated in 1930 as the Uniform Crime Reporting (UCR) Program. The UCR data is used by the FBI to develop criminal statistics for law enforcement agencies throughout the country.

1.4.2. NIBRS is comprised of six segments (e.g., Administrative Segment, Offense Segment, Property Segment, Victim Segment, Offender Segment and Arrestee Segment) and 53 data elements.

1.4.3. Security Forces must input information from civilians who commit offenses on Air Force installations into NIBRS. (T-0)

#### **1.5. General Administrative Information.**

1.5.1. Assistance. The Field Assistance Service (FAS) provides assistance to Base Network Control Centers, Defense Mega Centers and users worldwide. MAJCOM or local FSA will create new user accounts. FSAs will be appointed via appointment letters signed by their commander and a signed copy of the DD Form 2875, *System Authorization Access Request (SAAR)*. A copy will be sent to the respective MAJCOM FSA and will be maintained IAW Air Force Records Disposition Schedule (RDS). (T-3)

1.5.1.1. Installations may have four FSAs to create and maintain user accounts. The primary and alternate FSAs at SF squadrons will have staff level access and overall responsibility of system use for the unit. (T-3)

1.5.1.2. If additional administrators are needed, submit a request in writing to the MAJCOM FSA, who will notify AFSFC/SFOP for approval. (T-3)

1.5.2. Contractors hired in an SF unit in a capacity requiring access to SFMIS are authorized to be an FSA. They must complete the same requirements for training and authorization to use the system as military personnel and DoD employees. (T-0)

1.5.2.1. Contractors outside of this requirement are not authorized unless approved in writing by AFSFC/SFOP. MAJCOMs will provide a copy of appointment letters to AFSFC/SFOP, as well as a signed copy of the DD Form 2875. (T-0)

1.5.2.2. Prior to foreign nationals being authorized access to and use of Information Systems (ISs), they must meet the requirements IAW AFI 33-200, *Information Assurance Management*; AFI 31-501, *Personnel Security*; and AFSSI 8522, *Access to Information Systems*. This includes the AF provisioned portion of the Global Information Grid (GIG) (e.g., unclassified base LAN). (T-0)

1.5.3. FSAs will only have access to the “System Administrator” module in SFMIS. They must create another account to have access to the other modules without FSA rights. **NOTE:** Group accounts are NOT authorized. (T-0)

1.5.4. Wing/Support Group Commanders, Staff Judge Advocate, AFOSI and Military Equal Opportunity staff may request “live” access to SFMIS. These organizations may be given read only access with DFC’s Approval. Approvals must be in writing and maintained for record. (T-2)

1.5.5. SFMIS is Common Access Card (CAC) enabled. In order to access SFMIS with a CAC card, it must be done through the AF Portal. The CAC card can only be associated with one user name. If multiple user names are required for your duty position, then users will be assigned user names/passwords for access and permissions commensurate with “the need to know” information within the system. **Individual passwords will not be shared with other users.** It is a system security violation for multiple users to share the same user ID and password. Passwords will be changed at least every 60 calendar days, immediately upon compromise or after 45 days of inactivity. SFMIS can identify the number of days remaining until a change of password is required. Audits of the system will be done annually for proper accountability to prevent misuse/abuse of the system and data. (T-1)

1.5.6. Should a lockout occur as a result of an improper or forgotten password, the MAJCOM or unit FSA will assign a new password; however, the account will remain locked for a period of one hour or until the user’s identity can be positively identified. Users who have expired accounts must have their passwords reset through the functional system administrator. If after duty hours, contact the AFPEO BES/Field Assistance Service (FAS) Team 5 at DSN: 312-596-5771/COMM: 334-416-5771 then select option #1, then select option #5 and then option #4. If requesting assistance through the AFPEO BES/FAS, requestors will need to provide the FAS with an email with their SFMIS account user name, unit and DSN number. MAJCOM FSAs can perform this function for unit FSAs. Unit FSAs can perform this function for members of their unit. Problems encountered should be forwarded to the AFPEO BES/FAS for resolution. If a problem cannot be resolved within a reasonable time (24 hours), ensure the user gets a trouble ticket from the FAS, which will be forwarded to the SFMIS Program Manager’s office, until the problem is fixed. If users experience log-in problems due to their CAC, please refer to local procedures to unlock CACs.

**1.6. Privacy Information.** All SFMIS data is protected by the Privacy Act and must be handled as For Official Use Only (FOUO). All information will be strictly controlled IAW AFI 33-332, *Air Force Privacy and Civil Liberties Program*, to ensure it is only released to officials with a need-to-know. **Individuals may access SFMIS for authorized, official purposes only.**

**Military members who improperly access SFMIS or its information or provide or enable such access to third parties, for other than official authorized purposes, may be punished under Article 92, Uniform Code of Military Justice (UCMJ), and provisions of federal or state law. Civilian personnel who improperly access SFMIS, its information, provide, or enable such access to third parties, for other than official, authorized purposes, may be prosecuted under applicable provisions of federal or state law.** Violations by military or civilian members may result in the full range of authorized administrative and disciplinary actions in addition to otherwise applicable criminal or civil sanctions for violations of related laws. (T-0)

1.6.1. All SFMIS users are required to read the SFMIS Rules of Behavior pertaining to their tasks of safeguarding SFMIS information and sign the Acknowledgment of Responsibilities. All units will keep the Acknowledgement of Responsibilities for personnel on file. A copy of the Acknowledgement of Responsibilities can be found on USAF Security Forces SMARTNet NIPR- <https://afsfmil.lackland.af.mil>. Units can use this form or a locally generated memorandum that includes the same information to meet this requirement. (T-1)

1.6.2. Units will maintain signed Acknowledgement of Responsibilities on file while SFMIS user accounts are active. When SFMIS user accounts are no longer active, the letter will be archived IAW the Air Force Records Disposition Schedule (RDS). (T-1)

1.6.3. All SFMIS users must be aware that data displayed on monitors may be susceptible to unauthorized viewing. Take appropriate action to ensure privacy data is always protected. (T-0)

1.6.4. Violations of the system's operation or unauthorized release of the "FOUO" information will be immediately reported to the local FOIA office and Unit FSA, who will notify the commander at each level of concern. (T-0)

**1.7. SFMIS Capabilities.** SFMIS operates through the use of role-based access, granted to authorize users at all levels in the System Administration Module. The list below is not all inclusive and more features are added with each SFMIS release. Currently, the SFMIS program has the following capabilities:

1.7.1. Case Reporting, Accidents, Tickets (principal module for reporting DIBRS).

1.7.2. DEERS search, Suspension/Revocation/Debarment (SRB) Roster, case search and a history search.

1.7.3. Limited Confinement (to be DIBRS compliant). Tracking DIBRS-reportable information, inmate release dates, pre-trial/post-trial confinement and victim notification.

1.7.4. System Administration. Creating accounts and adding roles. **NOTE:** If you have an FSA account, the only module you can access with the FSA user name is the System Administrator Module.

1.7.5. Pass & Registration. Issuance of Restricted Area Badges (RAB). If DBIDs is off-line or not available at that location, visitor passes can be made by SFMIS or AF Form 75, *Visitor Pass*.

1.7.6. Combat Arms. Inputting training requests, class assignment, weapons course fired, AF Form 522, *USAF Ground Weapons Training Data*, history and supply account and tracking weapons via AFTO 105, Inspection Maintenance Firing Data for Ground Weapons.

1.7.7. Armory. Placing weapons/munitions/equipment in inventory, tracking weapon issues and the authority to bear arms.

1.7.8. Oracle “Discover Viewer”. The primary capability is searching for statistics which offers parameter setting for ad-hoc queries.

1.7.9. AFSFC/SFOP periodically publishes information regarding SFMIS. This information will appear on the SFMIS “Message of the Day,” SMARTNet and/or be posted on periodic electronic news releases. These messages inform users of developments, new releases and other important information. Users should check these sources for updates daily, and are highly encouraged to submit items to AFSFC/SFOP for future publication.

**1.8. On-Line Manual.** The SFMIS program has an online help manual available for users. The manual is user-friendly and can be printed for easy reference. Refer to DoD Instruction 7730.47-M Volume 2 for the DIBRS/NIBRS code tables. **NOTE:** These code tables are subject to change. DMDC controls the additions/deletions on the code tables.

**1.9. SFMIS Training.** The DFC must ensure personnel are trained to use SFMIS to meet installation needs and DIBRS requirements. Training and familiarization will not be conducted using the SFMIS “live” system modules. (T-1)

1.9.1. Web-Based Training (WBT). The SFMIS WBT module provides familiarization and refresher training. It is the primary means for familiarization training. WBT can be found on the SF SMARTNet. The primary capability is an interactive step-by-step process for each module on SFMIS.

1.9.2. Help Center. The SFMIS Help Center page provides useful information regarding everyday use of the SFMIS program. The Help Center is broken into five categories:

1.9.2.1. Contact Info. This page provides contact information for the FAS, MAJCOM and SFMIS Points of contact (POC).

1.9.2.2. Important Settings and Configuration. This page provides information regarding settings, basic trouble shooting, system requirements, signature pad, RAB and digital camera set up.

1.9.2.3. Information. This page provides information regarding development, frequently asked questions, login and password, known problems and quick How to Guides.

1.9.2.4. Context Sensitive Help. This page provides quick descriptions of fields in each module and serves as a compliment to the User Guides located in the Tutorials section.

1.9.2.5. Tutorials. This section provides User Guides for numerous topics in each SFMIS Module.

**1.10. Erroneous Incident Report Entries (EIRE).** If erroneous information is entered into the SFMIS “live” site, users need to notify the S5R or their FSA. S5R will then notify the DFC and MAJCOM FSA of the EIRE prior to voiding/deleting information. After contact is made with the MAJCOM FSA, the following steps should be conducted to correct the EIRE: (T-1)

1.10.1. The affected unit’s DFC or delegate will contact the servicing Staff Judge Advocate (SJA) regarding the EIRE and request a memorandum acknowledging the EIRE. The SJA will accomplish a memorandum acknowledging the voiding/deleting of the EIRE, which will be forwarded to the unit’s S5R and the MAJCOM FSA. The MAJCOM FSA will then

forward the completed memorandum to AFSFC/SFOP. Both MAJCOM and the local unit must maintain a copy of the memorandum. (T-1)

1.10.2. After the memorandum has been received by the unit's S5R, they must locate and open the erroneous incident report(s).

1.10.3. S5R will then delete all personal information from the report and enter a brief synopsis, concerning the reason for deletion in the narrative portion of the incident report panel and click the "Save" button. (T-1)

1.10.4. After completing the above actions, user will click on the "Routing" button in the incident panel to open the SFMIS Routing Dialog.

1.10.5. Select "Voided" from the "pick list" and be sure to click the "Save" button.

### **1.11. Requests for SFMIS Information and Releasing SF Information to the Public.**

1.11.1. IAW DoDI 5505.17, Collection, Maintenance, Use and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities, daily law enforcement operations include collecting personal information on the public, which must be safeguarded according to DoD. Follow AFI 33-332, and DoD 5400.7-R AFMAN 33-302, *Freedom of Information Act (FOIA) Program*. (T-0)

1.11.2. All first party requests will be directed to the unit's S5R section; no other SF office will provide this information unless designated by the DFC in writing and those individuals have been trained IAW paragraph 1.11.3. All third party requests will be forwarded to the local FOIA office. Contact the FOIA office at the installation for further guidance and assistance. Individuals or agencies desiring copies of reports (to include enclosures) or Security Forces blotters will do the following: (T-3)

1.11.2.1. If the requester desires copies of statements, they must submit a request under the *Privacy Act* (AFI 33-332) or the *Freedom of Information Act*, as required by DOD 5400.7, as supplemented.

1.11.2.2. Insurance companies requesting case reports concerning clients will make the request in writing. Units will assess a fee per DOD Regulation, 7000.14-R, Volume 11a, *Reimbursable Operations, Policy and Procedures*. Company checks will be used and made payable to Base Finance and mailed to the local SFAR office. Turn over checks to Finance using DD FM 1131, *Cash Collection Voucher*. No fees are assessed to private individuals requesting information on incidents they were involved in unless copies exceed regulatory amounts. Consult DOD 7000.14-R for further guidance.

1.11.3. Responsibilities. Security Force members, whose jobs require routine work with and/or access to a System of Records, and other records containing PII, are responsible to: (T-0)

1.11.3.1. Complete specialized Privacy Act training annually to comply with AFI 33-332, in addition to Privacy Act Annual Refresher Training. Reports and Analysis (S5R) will obtain job-related training through their respective FOIA/PA offices to cover responsibilities and procedures when releasing information to the public. Training will be annotated in training records. (T-0)

1.11.4. Disclosing Information. Consult the Staff Judge Advocate, Public Affairs, and FOIA office before releasing any information concerning the government. (T-3)

1.11.5. First Party Requests. Are queries from a subject or designated representative asking for access to his/her Privacy Act records. Examples of first party requests are: Traffic accident reports, statements and reports that deal with the requester.

1.11.5.1. First party requesters or their designated representatives shall submit a signed written request for access to Privacy Act record(s). Those who accept these requests must verify the identity of the requester to avoid unauthorized disclosures. Verification of identity will depend upon the sensitivity of the requested records. Identity can be verified in a number of ways, to include visually face-to-face with proper identification.

1.11.5.1.1. If the first party requester, requests via a signed letter, telephone or email, one of the following must be included: Unsworn declaration: "I declare under penalty of perjury (if outside the United States, add "under the laws of the United States of America") that the foregoing is true and correct. Executed on (date) (Signature)" or a notarized statement.

1.11.5.2. All requests will be logged and recorded to include: name of the requesting individual, date of request and list of items given. The log will be filed and recorded IAW AF RDS. (T-2)

1.11.5.3. Response to all Privacy Act requests shall be made within 20 workdays of receipt. (T-0)

1.11.6. Third Party Requests. Individuals seeking information to include statistical information must send the request to the servicing installation FOIA office. The requester can go to <http://www.foia.af.mil/> for information on how to submit a request. **NOTE:** If an insurance company uses another company to request information, this is considered a third party request and must go through FOIA.

1.11.7. Government Agency Requests. The following are procedures for release of information:

1.11.7.1. S5R is authorized to release information within their installation and will coordinate with DFC before information is released. (T-3)

1.11.7.2. MAJCOMs are authorized to release information within respective units of responsibility.

1.11.7.3. HQ AFSFC is authorized to release AF information.

1.11.7.4. The DFC is authorized to determine information sharing with other government agencies for statistical reports, the requests must be submitted and recorded. Statistical information can be released but cannot have any PII information included in the report. If PII information is required, the request must be sent to the local FOIA office. (T-2)

1.11.7.5. Law enforcement agencies can request information with an official request to local installations or MAJCOMs. IAW Title 10 USC Chapter 18, Military Support For Civilian Law Enforcement Agencies, USA PATRIOT Act (P.L. 107-56), and AFI 31-

101, information sharing between intelligence and law enforcement agencies is authorized. Each request will receive DFC approval, and all requests will be recorded. (T-3)

1.11.7.6. : Requests for SFMIS data submitted by federal government agencies (outside of law enforcement activity) are also addressed as a functional use/official use request directly by the record Office of Primary Responsibility. Requests for SFMIS data submitted by a state or local agency (outside of law enforcement activity) should be sent to the local FOIA office for appropriate review and action. Police or government agencies (e.g. Drug Enforcement Agency, Recruiters, Family Advocacy) requesting information for official reasons will receive all requested information after the identity of the agency can be verified. Such requests must be made either in person upon proper identification or using official letterhead. The written request can be mailed, scanned/mailed or faxed. Ensure the requester is advised to include points of contact, mailing addresses and phone or fax numbers to ensure a prompt response. Ensure requesters are authorized release under the Privacy Act (AFI 33-332) before disclosing the information. The requester's letter will be attached to the case files/blotters for a matter of record. Responses can be mailed, emailed or faxed back. The unit will maintain a log to verify action was completed. For investigators conducting military/federal background checks, the local SF unit will establish local policy/guidance on how this information is requested by investigators and tracked by the local Reports and Analysis Clerk. Requests from any Federal agency are required to apply for requests through the proper channels and have a valid need to know. (T-2)

1.11.7.7. MAJCOMs and Installation Commanders/DFCs may pull their own statistics to obtain criminal patterns or brief personnel on criminal activity for their installations. If MAJCOMs or installations need information from other MAJCOMs or installations, they must request the information in writing to the location desired or contact HQ AFSFC/SFOP. Statistical information may not be released without AFNETOPS/CC approval. This does not prevent Installation Commanders/DFCs from using their own statistics to obtain criminal patterns or brief personnel on criminal activity in the local area of their installation. Statistics will not be released for unit, numbered AF, regional, or MAJCOM comparisons. While local commanders may desire this information for comparison purposes, this does not meet the System Security Access Agreement's requirement for a valid need to know in order to release SFMIS information. Improper release of information without a valid need-to-know may jeopardize continued SFS access to the SFMIS.

1.11.7.8. Any release of information regarding the technical aspects of the system itself, not data contained within, must be coordinated through 24 AF/CC. Contact HQ AFSFC/SFOP for additional guidance. If the government was involved in an incident or the situation might result in litigation against the government, consult the Staff Judge Advocate before the release of any information. (T-1)

1.11.8. Violation of PII Disclosure. IAW AFI 32-332, *The Air Force Privacy and Civil Liberties Program*, immediately report any suspected or confirmed breaches of PII to the United States Computer Emergency Readiness Team (USCERT) within one hour of the discovery. Also, report action to the local Privacy Act Monitor or Officer and provide a preliminary report to the installation Privacy Manager. (T-0)

1.11.9. FOIA Exemptions. The FOIA provides access to federal agency records (or parts of those records) except those protected from release by nine specific exemptions. For more information refer to <http://www.foia.af.mil/handbook/>.

1.11.10. Deleting Records. The Air Force Board for Correction of Military Records is the authority for SFMIS records deletions. Individuals can also have records deleted if they receive a legal order of expungement of records pertaining to a specific case(s). (T-1)

## Chapter 2

### DEFENSE BIOMETRICS IDENTIFICATION SYSTEM (DBIDS)

**2.1. Background.** DBIDS is a DoD-owned and operated system developed by the Defense Manpower Data Center (DMDC) as an identity management program for personnel access at DoD installations. It is a networked client/server database system designed to electronically verify the access authorization of personnel entering military installations by the use of barcode contact and contactless reader. The program supports the adding, retrieving, updating and displaying of information for individuals who require military installation access. The DBIDS software application is used to enter personnel information into a database, capture biometric information and retrieve that data and biometric information for verification and validation at a later time. DBIDS enhances the military Integrated Defense (ID) mission by helping to provide a safe and secure community. DBIDS is the Air Force Physical Access Control System (PACS). **NOTE:** Installation Access Control System (IACS) is a version of DBIDS and is known as IACS in USAFE.

2.1.1. Installation entry control information is contained in AFI 31-113, *Installation Perimeter Access Control*.

2.1.2. The system works in the Online (connected to LAN) and Offline (not connected to LAN) modes.

2.1.3. The offline function is utilized when the server connection is down and access to the database through a local workstation is required. The offline function works from information stored in the hard drive of the respective workstation or Access Control Point (ACP). Newly added information on vehicles or personnel registered in DBIDS will not be available until the workstation can synchronize the data for that local file.

2.1.4. Users will use the DBIDS computers and handhelds for intended purposes only. No attempts to modify the system or settings will be made. No software or games will be loaded onto the system. The computer will not contain any software that is not vital to the operating system. The computer equipment will not be moved or modified in any way without the approval of the Site Security Managers (SSM). Do not disconnect or power down workstations unless directed by DMDC helpdesk or SSM. Personnel will ensure all DBIDS equipment is protected from damage by following these guidelines: (T-3)

2.1.4.1. Do not place objects on the computers or peripherals such as the fingerprint scanner.

2.1.4.2. Do not place drinks and other liquids near the computer or peripherals.

2.1.4.3. Do not move dedicated DBIDS computers or peripherals unless approved by SSM.

2.1.5. Personnel will also follow recommended actions to ensure the system remains fully operational (i.e., leaving at factory recommended settings, etc.).

2.1.6. Units will not use the system to meet other local administrative needs (i.e., using debarment field for loss of AAFES privileges). The system is meant to be standardized across the AF and DoD. (T-0)

2.1.7. Units will develop changeover and a work order system for damaged or malfunctioning equipment. (T-3)

## **2.2. Responsibilities.**

2.2.1. AFSFC/SFOP: Develops guidance for DBIDS use and management.

2.2.2. AFSFC/SFX: Coordinates with DMDC to provide comprehensive project plans for implementation of technology and software upgrades. Identifies costs for DBIDS programs, which include: help desk, technical support, DBIDS equipment, sustainment, life cycle replacement and system upgrades.

2.2.3. MAJCOM/A7S:

2.2.3.1. Ensures bases are equipped with adequate amounts of DBIDS equipment and coordinates additional equipment requests through AFSFC.

2.2.3.2. Monitors scanning rates for each base to ensure continuous progress toward 100% scanning at all entry control points.

2.2.3.3. Establishes overarching guidance for DBIDS utilization, operational policy and training requirements and coordinates with AFSFC and DMDC, as directed.

2.2.3.4. Maintains continuity of the DBIDS program for all bases.

2.2.3.5. Attends biometric conferences; provides input and gathers information from all DBIDS as funding allows.

2.2.3.6. Coordinates with HQ AFSFC to provide comprehensive project plans for implementation of updated technology and software.

2.2.4. Defense Force Commander (DFC):

2.2.4.1. Integrates DBIDS into daily operations. (T-3)

2.2.4.2. Establishes specific DBIDS mission standards and procedures in local Operating Instructions (OI). (T-3)

2.2.4.3. Programs for DBIDS consumables to include: card stock, printer ink, laminate, etc. (T-3)

2.2.4.4. Establishes procedures to initiate Be On the Lookout (BOLO) alerts, emergency notification (e.g., Red Cross) or other alert status. (T-3)

2.2.4.5. Establishes procedures for the installation commander concerning the review of personnel flagged as debarred at different DoD installations or facilities. The process should mirror the debarment process used for other situations to ensure consistency; it must also be approved by the installation commander and be reviewed by the base SJA. (T-3)

2.2.4.6. Will determine who the Base Security Officer will be. This position is an additional duty within the unit and normally within the Pass and Registration section. (T-3)

2.2.4.7. Establishes accountability and security procedures to prevent theft or damage at operating locations and access control points. (T-3)

2.2.4.8. Identifies to Communication Squadron Commanders (CSC) the criticality of support for DBIDS operations and resolution of network problems affecting DBIDS operations. (T-3)

2.2.5. Operator Responsibilities:

2.2.5.1. All DBIDS operators are required to complete DD Form 2875, *System Authorization Access Request (SAAR)*, which verifies suitability for access to DBIDS systems. Sites will maintain the original SAAR IAW Air Force Records Disposition Schedule (RDS). (T-3)

2.2.5.2. DBIDS operators are responsible for protecting PII information in DBIDS, must receive PII refresher training annually.

2.2.5.3. Additional DBIDS operator security and general security responsibilities should be described in MAJCOM/unit manuals or operating instructions.

**2.3. Roles.** DBIDS utilizes a role based system for enrollment, with the exception of foreign nationals (FN). All specific technical explanations and applications of individual roles can be found in the DBIDS User Manual. The manual is installed on every DBIDS computer and can be found on the DMDC website.

2.3.1. Base Security Officer (BSO): The BSO is the central controller for DBIDS. Each base can have a maximum of two BSOs, appointed by the DFC. SSMs are typically the operators who control the designation of individual roles for day-to-day use. Each base can have a maximum of four SSMs. BSOs and SSMs will be appointed via the DD form 2875 provided by DMDC. The DD Form 2875 is the appropriate form to appoint BSOs and SSMs. This document is used for System Authorization Access Request. If more personnel in either role are required, submit written requests through appropriate command channels to AFSFC/SFOP. Delete personnel roles within 72 hours of PCS, retirement and separation. This should be added to each unit's out-processing checklist. If a BSO or SSM is under investigation, access to DBIDS will be suspended until the pending investigation is cleared. (T-3)

2.3.1.1. Serves as the installation subject matter expert for DBIDS.

2.3.1.2. Develops local policy in compliance with standards of this instruction, applicable local instruction, Air Force Instructions, DoD regulations, Federal and local laws regarding DBIDS, biometric collection, access authority, Privacy Act and release of information.

2.3.1.3. Develops training, with unit training, incorporating system use and installation access control. Training materials will be updated as needed and will be reviewed annually for updates. Train new personnel on DBIDS software and components as they are assigned. Ensure training is annotated on the AF Form 623a, On the Job Training Record-Continuation Sheet. (T-3)

2.3.1.4. Training will include the following at a minimum: (T-1)

2.3.1.5. Login procedures to include local (off-line) login.

2.3.1.6. Login at Visitor Control Center and how to identify online and offline status.

2.3.1.7. How to manually lookup personnel, scan ID cards and scan fingerprints.

2.3.1.8. How to initiate minor troubleshooting on the DBIDS equipment, to include:

- 2.3.1.8.1. Failed login.
- 2.3.1.8.2. Network connectivity indicators.
- 2.3.1.8.3. Wireless connection.
- 2.3.1.8.4. PDA Configuration.
- 2.3.1.8.5. Helpdesk procedures.

2.3.1.9. Coordinates/reports all DBIDS major issues covered and not covered within this instruction with MAJCOM/A7SO.

2.3.1.10. Maintains accountability and reports any thefts or damages at operating locations and access control points. (T-3)

2.3.2. Site Security Manager (SSM): Provides a detailed report on all derogatory information received on an individual to the DFC or their designee and flags ID card holder's account. (T-3)

2.3.2.1. Ensures debarment, driving suspension/revocation information is input into DBIDS once notified by S5R. (T-3)

2.3.2.2. Maintains responsibility for the destruction of the old DBIDS Access Card (DAC), safeguards used DBIDS card printer ribbons and transfer film panels until properly disposed. Also responsible for removing printer ribbons and transfer film panels before printer is shipped for repairs or has been selected for DRMO. (T-3)

2.3.2.3. Provides quality control for data integrity on data input and randomly monitors registrar operations for quality and consistency. (T-3)

2.3.2.4. Performs user maintenance on all DBIDS equipment to keep them in proper working order and not exceed warranty recommended maintenance procedures; will also notify DMDC DBIDS contractors and the helpdesk where normal maintenance has not resolved component problems. (T-3)

2.3.2.5. Performs helpdesk procedures on DBIDS workstations and laptops prior to shipping an inoperable system for repairs. (T-3)

2.3.2.6. Ensures equipment is not shipped for repair without a DMDC Helpdesk ticket number. Do not ship for 24 hours, as a DMDC Helpdesk representative may call to further diagnose the problem. If DMDC does not call within 24 hours and a ticket number is available, ship the item. The DMDC Helpdesk can be reached via Toll Free Number: 1-800-372-7437. (T-3)

2.3.2.7. Keep track of all DBIDS consumable supplies (i.e., ink or ribbon, laminate and card stock). Attempt to limit ordering to annually (preferably July-September). (T-3)

2.3.2.8. Provide support to flight operations during initial trouble calls with DBIDS equipment prior to contacting the DBIDS Help Desk. (T-3)

2.3.2.9. Maintain points of contact with base Communications Squadron for network issues concerning (DBIDS) connectivity. (T-3)

**2.4. System Integration.** The integration of DBIDS into daily installation access control procedures aids the prevention of unauthorized access to the installation by providing the capability to:

- 2.4.1. Detect attempts to access installations using forged, invalid or unauthorized access documents/credentials.
- 2.4.2. Query a database for information on individual access privileges that is networked to Air Force installations.
- 2.4.3. Provide centralized control of access privileges (for example, commanders may withdraw a terminated employee's access authorization).
- 2.4.4. Scan (contact or contactless) Personal Identity Verification (PIV) authorized credentials, Department of Defense identification (DoD ID) cards and DBIDS produced IDs to verify access authorization and privileges.
- 2.4.5. Maintain an automated historical record of personnel who have accessed the installation.
- 2.4.6. Receive immediate notification when a barred individual attempts to enter the installation.
- 2.4.7. Support Force Protection Condition (FPCON) measures related to installation access control.

## **2.5. System Operation.**

- 2.5.1. Installations with DBIDS must utilize the system IAW AF 31-113. (T-2)
- 2.5.2. Traffic lanes at the installation gates will be equipped with DBIDS scanners. (T-2)
- 2.5.3. Visitor Control Centers should be equipped with DBIDS desktop computers to facilitate issuing visitor passes and generate daily reports (if required).
- 2.5.4. Base Defense Operations Centers (BDOC) may have DBIDS computers and personnel with law enforcement officer (LEO) access. This facilitates the ability of BDOC personnel to find information on those individuals in DBIDS. There are also unique functions the LEO role can perform. Specifics on these functions can be found in the DBIDS manual.
- 2.5.5. ID cards will be scanned by using a handheld device. An audible beep and a green light will verify the ID card has been scanned properly. If the handheld will not scan the ID cards, scan them with the pistol scanner attached to the gate system. The purpose is to verify if there is a problem with the ID cards. If problem continues, conduct a manual lookup on the computer desktop. Instruct the person to report to the Visitor Control Center (VCC) to assist in resolving any problems.
  - 2.5.5.1. The scanner will positively identify an individual and return an access recommendation (green, yellow or red).
  - 2.5.5.2. If a green screen appears, physically verify the individual's picture and information on the ID card against the display and person presenting the ID.

2.5.5.3. If the information matches, allow entry. If it does not match, deny entry and send for secondary screening. BDOC will be contacted immediately if the secondary screening does not match.

2.5.5.4. If a yellow screen appears, it can indicate, but is not limited to, any of the following: debarred at another installation, driving status suspended, Red Cross notifications or pending DEERS verification. Check Status box on handheld scanner for information.

2.5.5.5. If a red screen appears, follow the displayed instructions. Red notifications will normally consist of: wants and warrants, Be On The Look Out (BOLO), barred, call law enforcement, expired ID, terminated ID, lost or stolen, unrecognized credential, unauthorized credential, not authorized at this time/day/gate, etc. Check Status box on handheld scanner for information. Access Point Operators must pay attention to the notifications which will clearly detail the reason for a red screen. Use of Force may be required with certain notifications.

2.5.5.6. Yellow and red notifications will require action. Units should develop procedures for handling these notifications.

2.5.6. If the individual is not registered in DEERS, the individual will be required to go to the installation's designated visitor center and produce two forms of identification. Installations will determine the age required for children to receive a DBIDS credential and if they have to be registered in the system. Circumstances for how this is applied will be developed locally.

2.5.7. In the event of a lost or forgotten identification card, personnel can gain access to the installation with a sponsor or issuance of a pass after authentication of fingerprints or the card can be brought to the member prior to being allowed entry.

2.5.8. Individuals must be registered in DBIDS at an installation in order to facilitate access. DBIDS v.4.0. will automatically register personnel with CAC or Teslin ID cards when the ID is scanned with the handheld scanner at the ACP, or the ID may be manually registered at the VCC. Non DoD PIV cardholders, FNs, DBIDS cardholder and visitors must be manually registered in DBIDS.

2.5.9. Actions for System Failure. Any technology can fail for a number of reasons. In the event the DBIDS system is off line and credentials cannot be produced, the AF Form 75 and SFMIS will be used to allow access IAW AFI 31-113.

### Chapter 3

#### NATIONAL LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEM (NLETS)/NATIONAL CRIME INFORMATION CENTER (NCIC) AND ADDITIONAL SYSTEMS

**3.1. Program Definition.** National Law Enforcement Terminal System (NLETS) and National Crime Information Center (NCIC) are access systems to civilian law enforcement data. These systems allow the prompt exchange of law enforcement information between Security Forces and other law enforcement officials. NLETS/NCIC terminals are required for identity verification prior to issuance of visitor passes/DBIDS Cards. Potential locations for NLETS/NCIC to support DBIDS operations are the Visitor Control Centers, 24 hour SF Facility (BDOC) to conduct name checks after the Visitor Center closes and the Commercial Vehicle Inspection (CVI) station. As indicated below, the DFC will determine the number/location of NLETS/NCIC terminals needed to accomplish identity verification.

**3.2. Program Responsibilities.** The following agencies and personnel are responsible for various aspects of the NLETS/NCIC program:

3.2.1. HQ AFOSI is the US Air Force executive agency for National Crime Information Center (NCIC) matters.

3.2.2. MAJCOMs ensure US Air Force installations in the same state share systems and fund system acquisition, installation and support.

3.2.3. The DFC establishes the need for an NLETS/NCIC terminal(s) and before acquiring and installing s/he must: (T-0)

3.2.3.1. Contact MAJCOM/A7S to identify/obtain the FBI assigned ORI for the SF unit. Then contact the host state system administrator and coordinate actions required to become part of the state's system through a dedicated terminal.

3.2.3.2. Determine the initial cost, to include procurement of power conditioning and continuation interfacing equipment (PCCIE).

3.2.3.3. Determine recurring costs of terminal equipment.

3.2.3.4. Receive PCCIE guidance from the base civil engineer.

3.2.3.5. Coordinate local funding for servicing equipment with base agencies.

3.2.3.6. Coordinate with the base contracting officer to develop a service agreement.

3.2.3.7. Determine facility protection and environmental requirements to satisfy state requirements for terminal installation.

3.2.3.8. Coordinate with the base civil engineer squadron for the necessary building repairs or modification requirements to accommodate NLETS/NCIC.

3.2.3.9. Coordinate with the base communications squadron to ensure necessary equipment and capabilities exist.

3.2.4. The DFC is also responsible for training; the following are required: (T-0)

- 3.2.4.1. Coordinates and establishes training requirements for local operators with the state terminal authorities. (T-0)
- 3.2.4.2. Ensures the training meets state and FBI requirements. (T-0)
- 3.2.4.3. Ensures training of selected persons in terminal operation. (T-0)
- 3.2.4.4. Ensures only trained and qualified persons operate the terminal. (T-0)
- 3.2.4.5. Ensures proper documentation of training records. (T-0)
- 3.2.4.6. Terminates operator access privileges for misuse of NCIC terminals. (T-0)

**3.3. Providing System Protection.** Restrict access to data as “OFFICIAL USE ONLY Law Enforcement Sensitive”. Users and serviced agencies follow the state and NCIC guidance on policies, procedures, formats and codes required for entering records into the system. Users of the system can include but are not limited to SF members, Department of the Air Force (DAF) Civilian Police and DAF Security Guards requiring an official need for the information. (T-0)

**3.4. Criminal History Data.** Computerized Criminal History (CCH) and the NCIC Interstate Identification Index (III) are federal systems of records and are controlled under the Privacy Act of 1974. Grant access to this data for valid law enforcement purposes on a case-by-case basis. There must be a DFC level approval process involved with access. Units will determine the process and codify it in local instructions. (T-0)

3.4.1. Requests from outside the SF unit, with the exception of AFOSI, must be in writing and include the reason for the request to be approved by the DFC. Disclose data according to AFI 33-332 and Chapter 2. (T-0)

3.4.1.1. NCIC name checks are authorized for all visitors entering the installation. Refer to AFI 31-113 for more information.

3.4.1.2. Positive “Hit” for Code 4/Wants and Warrants: (T-0)

3.4.1.2.1. The operator of the system must ensure privacy is adhered to at all time and all radios are secured and away from the subject before any information can be transmitted across the net.

3.4.1.2.2. Any agency that receives a record in response to an NCIC inquiry must confirm the “hit” on the record. Hit confirmation must be made prior to taking any action based upon the hit, such as arresting the wanted person, detaining the missing person, or seizing the stolen property. Once the Security Forces Controller receives the initial notification of a hit, he will then direct the patrolman to “secure their mics”. This warning will advise the patrolman to turn their radio down and of possible danger/criminal history of their subject. Also, this will ensure the radio transmission is not overheard by the vehicle occupants and alerting them of a possible warrant situation. While receiving the information, the patrolman will take appropriate measures to get behind the vehicle for an additional layer of cover. Simultaneously, the SF Controller will direct another patrol to respond Code 2 to assist the patrolman on scene. Once an additional patrolman is on scene, they will take appropriate actions to detain the subject unit the situation is resolved.

3.4.1.2.3. Confirming a hit means to contact the agency that entered the record to ensure that the person or property inquired upon is identical to the person or property identified in the record.

3.4.1.2.4. Ensure that the warrant, missing person report, or theft report is still outstanding. Obtain information regarding: (1) the extradition of a wanted person when applicable, (2) the return of a missing person to the appropriate authorities, (3) the return of stolen property to its rightful owner, or (4) the terms and conditions of a protection order.

3.4.1.2.5. NLETS is the recommended network for Hit confirmation. Even if the initial confirmation is handled via telephone, NLETS should be used for documentation. NLETS has created inquiry (YQ) and response (YR) formats for Hit confirmation. The (YQ) must contain one of the following priorities:

3.4.1.2.5.1. Priority 1/Urgent - confirm the hit within 10 minutes. This priority should be used in those instances where the Hit is the only basis for detaining a suspect or the nature of a case requires urgent confirmation of a hit.

3.4.1.2.5.2. Priority 2/Routine - confirm the hit within 1 hour. This priority will be used when the person is being held on local charges or when property has been located under circumstances where immediate action is not necessary. **NOTE:** After confirming the hit with the entering agency and upon taking a person into custody or acquiring property, the recovering agency must place a "locate" on the corresponding NCIC record. This will indicate to initiating law enforcement agency the subject or property location.

3.4.2. Although this is not a background check, it will provide feedback on whether the person is wanted by any federal agency, to include the national Terrorist Screening Center (TSC) IAW AFI 31-113. A positive hit, via the TSC, will provide the following information in most circumstances: (T-0)

3.4.2.1. Handling Code 1:

**Table 3.1. Handling Code 1.**

\*\*\* LAW ENFORCEMENT SENSITIVE INFORMATION \*\*\*

WARNING – APPROACH WITH CAUTION

THIS INDIVIDUAL IS ASSOCIATED WITH TERRORISM AND IS THE SUBJECT OF AN ARREST WARRANT, ALTHOUGH THE WARRANT MAY NOT BE RETRIEVABLE VIA THE SEARCHED IDENTIFIER. IF AN ARREST WARRANT FOR THE INDIVIDUAL IS RETURNED IN YOUR SEARCH OF NCIC, DETAIN THE INDIVIDUAL PURSUANT TO YOUR DEPARTMENT'S PROCEDURES FOR HANDLING AN OUTSTANDING WARRANT, AND IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER (TSC) AT (866) 872-9001 FOR ADDITIONAL DIRECTION.

IF AN ARREST WARRANT FOR THE INDIVIDUAL IS NOT RETURNED, USE CAUTION AND IMMEDIATELY CONTACT THE TSC AT (866) 872-9001 FOR ADDITIONAL

DIRECTION WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.

UNAUTHORIZED DISCLOSURE OF TERRORIST WATCHLIST INFORMATION IS PROHIBITED. DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST. INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY THAT MAY NOT BE DISSEMINATED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

\*\*\*LAW ENFORCEMENT SENSITIVE INFORMATION\*\*\*

#### 3.4.2.2. Handling Code 2:

**Table 3.2. Handling Code 2.**

“\*\*\* LAW ENFORCEMENT SENSITIVE INFORMATION \*\*\*

WARNING – APPROACH WITH CAUTION

THIS INDIVIDUAL IS OF INVESTIGATIVE INTEREST TO LAW ENFORCEMENT REGARDING ASSOCIATION WITH TERRORISM AND THERE MAY BE A DETAINER AVAILABLE FROM THE DEPARTMENT OF HOMELAND SECURITY FOR THIS INDIVIDUAL.

IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER AT (866) 872-9001 OR, IF YOU ARE A BORDER PATROL OFFICER, IMMEDIATELY CALL THE NTC TO ASCERTAIN IF A DETAINER IS AVAILABLE FOR THE INDIVIDUAL AND TO OBTAIN ADDITIONAL DIRECTION. PLEASE QUESTION THIS INDIVIDUAL TO ASSIST THE TSC IN DETERMINING WHETHER THE INDIVIDUAL ENCOUNTERED IS THE SUBJECT OF A DETAINER WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER.

UNAUTHORIZED DISCLOSURE OF TERRORIST WATCHLIST INFORMATION IS PROHIBITED. DO NOT ADVISE THE INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST. INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS PROPERTY OF THE TSC AND IS FEDERAL RECORD PROVIDED TO YOUR AGENCY THAT MAY NOT BE DISSEMINATED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCED AUTHORIZATION OF THE TSC.

\*\*\*LAW ENFORCEMENT SENSITIVE INFORMATION\*\*\*”

## 3.4.2.3. Handling Code 3:

**Table 3.3. Handling Code 3.**

“\*\*\*LAW ENFORCEMENT SENSITIVE INFORMATION\*\*\*

DO NOT ADVISE THIS INDIVIDUAL THAT THEY MAY BE ON A TERRORIST WATCHLIST.

CONTACT THE TERRORIST SCREENING CENTER (TSC) AT (866) 872-9001 DURING THIS ENCOUNTER. IF THIS WOULD EXTEND THE SCOPE OR DURATION OF THE ENCOUNTER, CONTACT THE TSC IMMEDIATELY THEREAFTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.

ATTEMPT TO OBTAIN SUFFICIENT IDENTIFYING INFORMATION DURING THE ENCOUNTER WITHOUT OTHERWISE EXTENDING THE SCOPE OR DURATION OF THE ENCOUNTER, TO ASSIST THE TSC IN DETERMINING WHETHER OR NOT THE NAME OR IDENTIFIER(S) YOU QUERIED BELONG TO AN INDIVIDUAL IDENTIFIED AS HAVING POSSIBLE TIES WITH TERRORISM.

DO NOT DETAIN OR ARREST THIS INDIVIDUAL UNLESS THERE IS EVIDENCE OF A VIOLATION OF FEDERAL, STATE OR LOCAL STATUTES.

UNAUTHORIZED DISCLOSURE IS PROHIBITED.

INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

WARNING – APPROACH WITH CAUTION

“\*\*\*LAW ENFORCEMENT SENSITIVE INFORMATION\*\*\*”

3.4.2.4. All of the codes listed above are currently going out to agencies that utilize NCIC. Information from the TSC can be found on the Security Force SMARTNet at <https://afsfmil.lackland.af.mil/>. Units must ensure they have policies on how to handle these situations. Immediately contact local AFOSI on all TSC “hits”. AFOSI will coordinate with local FBI JTTF on plan of action. Coordinate with the local AFOSI on standard operating procedures to be utilized for each tier of TSC “hit”. Do not enter Subject’s name and identifiers into a blotter entry or into SFMIS. AFOSI investigates terrorism cases jointly with the FBI and is the primary liaison agency for the Air Force with the FBI and other federal agencies. FBI investigative data will not be entered into other data bases (SFMIS) or permanent documents (SF Blotters) due to discovery actions that could impact the investigations. Additional agreements must be in place to define

how these scenarios will be handled after notification of AFOSI and subsequently the FBI.

3.4.2.5. TSC information and local policy must be included in annual training and Duty Position Evaluations (DPE) for all positions which may receive TSC notifications via NCIC or through notification. This will include the following positions: Desk Sergeant, Flight Sergeant, Visitor Control Center, Installation Entry Controller and others. (T-0)

3.4.3. Prohibit obtaining the CCH or NCIC III data from other sources except as authorized by the installation DFC. (T-3)

3.4.4. Keep all requests for CCH or NCIC III check data from outside the SF unit on file for validation purposes. If validation records do not correspond with access-approval files, conduct an inquiry to resolve the difference. (T-3)

**3.5. Validation System and Records Maintenance.** Validate all entries into NCIC III or State Terminal System (STS). The FBI or STS sends records that require validation to the DFC. The DFC establishes a validation system that includes:

3.5.1. Security Forces Desk Blotter (AF Form 53) entry or an Incident Report (AF Form 3545A) containing complaints where the offense occurred. This serves as source documents for entries.

3.5.2. Use a folder for NLETS or NCIC-directed validation documents to maintain a list of all system entries.

3.5.3. The Defense Force Commander must select a terminal agency coordinator (TAC) to supervise, train with and control terminal operations. The TAC uses available documentation to validate entries into the system. (T-3)

**3.6. Agencies Receiving NLETS/NCIC Service.** Agencies will adhere to the written requirements and responsibilities provided by the terminal-owning agency. Written requirements include training, physical protection and validations. Units with NLETS service will appoint a primary and alternate system administrator. Administrators should be appointed in the section which oversees routine use of the system, generally the S3 section. (T-0)

**3.7. Additional SF Systems.**

3.7.1. ForcePRO is a software application and the only authorized automated tool to conduct the Integrated Defense Risk Management Process (IDRMP). ForcePRO was developed to relieve the risk analyst of a large number of hand calculations while considering the risks to assets numbering in the tens to hundreds (specifically an entire AF base). ForcePRO is an AF certified Decision Support Tool authorized to be installed on AF computer systems connected to the AF Global Information Grid (GIG). Once data is input into ForcePRO, the information contained within becomes classified and must be safeguarded. For more information on ForcePRO and the IDRMP, refer to AFI 31-101.

3.7.2. The Security Forces SMARTNet is a conceptual approach to the future management of Security Forces web-based computer applications. In the past, applications were developed either by the unit, the Major Command or the Headquarters Air Force Security Forces Center when units established and validated new requirements. The programs were normally contracted as stand-alone applications. This resulted in a multitude of programs with unfamiliar user interfaces, disparate databases and no common code base.

3.7.2.1. SMARTNet is intended to consolidate programs to the greatest extent possible to maximize efficiency and reduce resource allocation. Where possible, technicians will re-write programs to a common programming language and use a mutual database on a supported platform. This will ensure efficiencies are realized in re-utilization of common application code, reduce manpower by utilizing shared programming skill sets, condense cost as a result of corporate software procurement and increase security for critical law enforcement personally identifying information (PII) data. Additionally, by streamlining the DoD certification and accreditation process and simplifying the migration to evolving technologies, applications can become more robust and released back to the user sooner.

3.7.2.2. Where possible, merging programs onto common hardware platforms will reduce hardware costs (servers, switches, UPS, etc.), decrease manpower costs for system administration, lower server hosting costs and increase stability while guaranteeing increased uptime. This will aid in future technological advancements of the Security Forces career field by allowing the deployment of automated products, reducing the training time to learn new programs and more efficient use of valuable resources.

3.7.3. The Working Dog Management System (WDMS) is a software program developed for the DoD Military Working Dog (MWD) Program and is utilized by the 341 TRS, Military Veterinary Services, US Air Force, Marine Corps, Navy and US Army MWD management offices. WDMS provides full lifecycle management of the identity, medical status, training, operational assignment and disposition of military working dogs that have been evaluated, acquired and deployed by the DoD and other Federal agencies participating in the program. The system now maintains over 10,000 dog records and other supporting records.

3.7.3.1. To reach the worldwide customer base, the system is web based operating on a framework permitting worldwide access via the Internet and local area networks (LANs) using Secured Socket Layer (SSL) and encryption technologies. Data entry, reporting and ad-hoc querying can be performed. The application is composed of autonomous modules operating off a common database. Each module facilitates a business function that generates or uses information significant to the lifecycle management of a working dog. This system is managed by the DoD MWD Program Manager at HQ AFSFC and is accessible via SMARTNet.

## Chapter 4

### SECURITY FORCES FORMS

**4.1. AF Form 52, Evidence Tag.** Use this two-part form to record receipt or seizure of evidence or other acquired property and maintain a chain of custody. The disposal of all evidence will be coordinated through the SJA. (T-2)

**4.2. AF Form 53, Security Forces Desk Blotter.** The BDOC/Emergency Control Center (ECC) controller prepares this form as the official chronological record of Security Forces activities. Installations with more than one BDOC/ECC, must complete separate blotters. Completed AF Forms 53 should include sufficient information to identify persons concerned, time of incident, facts and circumstances of incidents, and provide a complete summary of events for the duty shift of each flight. The form will be initiated at the beginning and terminated at the closing of each duty shift. Blotters must be signed by the on-duty flight sergeant to certify the form is official. Ensure required information is included on the reverse side of the original copy. Units may create alternate Microsoft Word versions of the AF Form 53. Local generated products must comply with AF RDS and PII rules and regulations. AF Forms 53 often contain sensitive investigative or Privacy Act information and must be controlled.

4.2.1. Blotters may be kept electronically. If filed electronically, MAJCOMs/local installations will develop a system to ensure the blotters are being reviewed by the Flight Leader/Flight Sergeant.

4.2.2. Prepare sufficient copies to satisfy local requirements; however, distribution must be limited to only those personnel who have a valid daily requirement to monitor it, such as the Wing Commander, the local AFOSI detachment and the SJA or as determined by the Installation Commander. At no time should the blotter be distributed below group level. Unit first sergeants and commanders receive notifications involving personnel within their unit. If the Installation Commander decides to add agencies or positions to the distribution list not listed here, it must be done in writing. The additional distribution list will be reviewed annually to ensure it is relevant.

**4.3. AF Form 75, Visitor/Vehicle Pass.** The AF Form 75 is an alternate means for controlling entry on and off AF installations if DBIDS or SFMIS are unavailable. This form is available on the e-publications website. This form is completed in two copies. Give the original (1st copy) to the individual and file the second copy.

**4.4. AF Form 1109, Visitor Register Log.** Provides a log of visitors/and or personnel entering areas which the entry and/or exit is controlled.

**4.5. AF Form 1168, Statement of Suspect/Witness/Complainant.** This form is to be used when taking a written statement from a suspect, accused person, witness or complainant (military or civilian). This form is also used to advise an individual of their Article 31/Fifth Amendment rights. As a minimum, mark the document "For Official Use Only." Sufficient copies should be prepared to satisfy local requirements.

**4.6. AF Form 1176, Authority to Search and Seize.** A search is an examination of a person, property or premises to uncover evidence of a crime or to uncover evidence of a criminal intent, such as stolen goods, burglary tools, weapons or other evidence. A seizure is the taking of such

items by authorities for evidence at a courts-martial or trial. Use the AF Form 1176 to ensure the search and seizure is legal and any evidence found is admissible at a courts-martial and Magistrate Court. This form is prepared for the signature of the commander having search authority over a specific area, property or person to be searched. The commander may give verbal authority to search only after a probable cause briefing to him/her is accomplished and the situation warrants immediate search. The commander must sign the AF Form 1176 as soon as possible after oral authorization. Once the form is signed, Security Forces will retain and place it into the case file. **NOTE:** Authority to Search and Seize is only valid for 3 days; if sufficient evidence is not collected within the 3-day time frame, a new 1176 needs to be accomplished. Copies are made and forwarded based upon local requirements. A search authorization is not a search warrant. Search warrants are an authority to search issued by civilian authorities only.

**4.7. AF Form 1199 Series of Restricted Area Badges.** The USAF Restricted Area Badge is issued to each person who is granted unescorted entry authority for restricted areas. The forms are serial numbered as well as accountable and supplies must be kept secured. The forms are self-explanatory and normally issued by the Pass and Registration Section. Refer to AFI 31-101 for additional guidance on these forms.

**4.8. AF Form 1313, Driver Record.** Use this form as a cumulative traffic record (driving history) for drivers who are principals in motor vehicle traffic accidents or moving traffic violations IAW AFMAN 31-116, *Air Force Motor Vehicle Traffic Supervision Program*.

**4.9. AF Form 1315, Accident Report.** This form is used to record investigations of major traffic accidents. The investigation of major accidents should be accomplished by a trained accident investigator. Refer to AFMAN 31-116.

**4.10. AF Form 1361, Pick-Up/Restriction Order.** This form is used to record facts and provide Security Forces with information about pick-up or restrictions on members of the military services. The BDOC/ECC controller is responsible for completing the form. Filling out the form is self-explanatory. In the remarks section, include a brief statement as to why the individual is restricted or required to be picked up.

**4.11. AF Form 1364, Consent for Search and Seizure.** This form is used when an individual voluntarily consents to a search of their person, area under their control or their personal possessions. Probable cause is not needed to ask a person for consent to search. Use this form to obtain the consent in writing. Also, ensure the suspect and witnesses to the consent sign the appropriate blocks on the form. Ensure the person giving consent reads and fully understands that anything found in the search can be used against them in a criminal trial, other judicial or administrative proceedings. Inform the individual that if they do not consent to a search, the Security Forces member cannot conduct a search without consent, authorization, warrant or other authorization recognized by law. Prepare this form only in one copy and then retain it with the case file.

4.11.1. If during the search the individual withdraws their consent, terminate the search immediately. Ensure all pertinent information (time consent withdrawn, time search terminated and actions taken) are documented in the AF Form 3545, *Incident Report*.

**4.12. AF Form 2586, Unescorted Entry Authorization Certificate.** This form is used to document, coordinate, and approve unescorted entry authority. **NOTE:** The IDP will list the units responsible for initiating the AF Form 2586.

**4.13. AF Form 3226, Authority to Apprehend in Private Dwelling.** Rule for Courts-Martial (RCM) 302 (e) of the Manual for Courts-Martial (MCM), requires written authority be obtained prior to apprehending a person in a private dwelling. This form is used to document receipt of this authority.

**4.14. AF Form 3545 and AF Form 3545(A), Incident Report.** The AF Form 3545 and 3545(A) were created to meet the requirements of NIBRS/DIBRS reporting as detailed in Chapter 1. Use this form to record facts about an incident or complaint for the proper military authority. Include in the report all available facts, names of personnel involved and a summary of the initial on-scene investigation.

4.14.1. Use the AF Form 3545 as the official Incident Report at sites where SFMIS is not available. In this case, each offender/victim/witness will require a separate information page. For example, there may be three offenders; each will require his/her own information page. At sites with SFMIS access, use the AF Form 3545 as a worksheet to gather all necessary information for future input into SFMIS and for creating the AF Form 3545(A).

**4.15. AF Form 3907, Security Forces Field Interview Data.** This form is used to record routine contact between Security Forces members and members of the public IAW. For example, if a suspicious person was observed walking around the housing area in the middle of the night, this form would be used to record the contact made with the individual. The form is completed in one copy and is forwarded to the Security Forces Investigations Section. The Investigations Section can then compare this form with reported crimes in the area to develop possible leads or suspects. The form is self-explanatory.

4.15.1. Units will develop guidance and procedures for the disposition of AF Forms 3907. (T-3)

**4.16. AF Form 4443, Law Enforcement and Physical Security Activities Report (LEPSAR).** This form is used to query statistics on all criminal activity and assist installation commanders to reduce crime.

**4.17. DD Form 460, Provisional Pass.** This form is issued by a Security Forces member to an enlisted member of the Armed Forces. Information required by the form is self-explanatory. The DD Form 460 is issued when:

4.17.1. The member is apprehended for a minor violation which does not require detention, but which may result in a delay preventing them from reporting to their assigned duty section/ installation within the time limit indicated on their orders or pass.

4.17.2. The member's previous pass has expired or he/she is without a pass or leave orders, but is en route to his/her destination as evidenced by a valid transportation ticket.

4.17.3. The member can present evidence they reported or attempted to report his/her delay to his/her commander.

4.17.4. Because of extenuating circumstances, the member missed their transportation, are delayed through no fault of their own and they voluntarily report their status to proper authority.

4.17.5. It is necessary to order an individual to return to their home station after apprehension for Absent Without Leave (AWOL).

**4.18. DD Form 1408, Armed Forces Traffic Ticket.** This form is issued to an individual who has committed a moving or non-moving traffic offense. It is prepared in three copies. The original (white) copy is submitted through channels to the violator's commander or if the violator is a military family member, to the sponsor's commander. If the violator is a civilian employee, the white copy is sent to the individual's commander. The ticket is sent to commanders for action to be taken against the violator. Unit Commanders or Section Commanders are the only personnel allowed to sign the Command Action area of the DD Form 1408, *Armed Forces Traffic Ticket*. Ensure this form is entirely completed.

4.18.1. The second (yellow) copy is used by Security Forces to record pertinent information. It can record details about the instructions issued to the violator, names of witnesses to the offense and vehicle defects. Tracking history for stationary and moving RADAR can also be detailed. Use this information later to refresh the patrol person's memory if the ticket is contested. The yellow copy is then filed in the S5R section.

4.18.2. The third copy (pink) is given to the violator or affixed to the vehicle if the vehicle is unattended. Do not complete blocks 2-7 if ticket is left on an unattended vehicle. This will ensure personal information is protected. The patrolman will still need to complete blocks 2-7 on the (white/yellow) copies for administration purposes. Complete the back of the pink copy before giving it to the violator. This gives the violator written reporting instructions. This must be done even if the violator has been given verbal instructions. Normally, the back of the pink copy is completed before the back of the yellow copy. This prevents the violator from being detained for an unnecessary amount of time.

4.18.3. File the second (yellow) copy and give the third (pink) copy to the violator or place it on the windshield of the unattended vehicle. If there is inclement weather, place the ticket in a plastic bag.

4.18.4. The reverse side of the DD Form 1408 is used for transmittal of traffic violations through military channels. Ensure the violation indicated on the DD Form 1408 is IAW AFMAN 31-116 and all required information is carefully entered on the form.

4.18.5. Ensure the required information is annotated. If the ticket has administrative errors, it will be returned to S3 for correction. If the ticket needs to be voided, the issuing Security Forces member or DFC may do so. No other person has the authority to void a ticket.

**4.19. DD Form 1920, Alcohol Influence Report.** This form is used to record field sobriety tests and observations made of individuals suspected of being involved in any incident where alcohol or drugs may be a factor. The apprehending Security Forces member will complete the form and it will become a record of their observations for future reference. Record all observations made, including those not required by the DD Form 1920.

**4.20. DD Form 2701, Initial Information for Victims and Witnesses of Crime.** This form should be available and is issued to all personnel when criminal conduct adversely affects victims or when witnesses provide information regarding criminal activity. If in doubt, issue the form. The form gives the individual information on the Victim/Witness Assistance Program (VWAP) and is self-explanatory. Information needed to complete the form can be obtained from the base legal office or the S2I. When the form is issued, it must be documented on AF Form 53 and AF Form 3545. Further information on the DD Form 2701 and the VWAP is contained in AFI 31-118, *Security Forces Standards and Procedures*.

**4.21. DD Form 2708, Receipt for Inmate or Detained Person.** This form is used when Security Forces personnel are releasing an individual they have detained or apprehended. It can also be used to transfer prisoners between confinement facilities. The form is self-explanatory and should be prepared in two copies. The original form is maintained with the case file as a source document indicating an official transfer of the individual and the copy is given to the individual who received the subject.

**4.22. United States District Court Violation Notice (USDCVN).** This form is used when it is determined an offender will be prosecuted for a minor offense before a US Magistrate under AFI 51-905, *Use of US Magistrates for Trial of Misdemeanors Committed by Civilians*. Active Duty Air Force personnel will not be issued a USDCVN. Security Forces, Department of the Air Force civilian guard/police or game wardens who are authorized to make an apprehension, arrest or to issue a violation notice or ticket, will issue this form. Before it is distributed, the specific address of the Clerk of the United States Court (Central Violations Bureau) to which the violator must address his/her communication will be stamped (or typed) in black ink, on the reverse of the violator's copy (manila card stock) of the four-part form. The USDCVN is accountable once it is issued to the violator.

4.22.1. When completing the USDCVN, Security Forces personnel must take great care to assure each entry is legible and no entry is smudged on the chemically carbonized paper copies. **NOTE:** Required information for the violation notice may vary from installation to installation. Consult with the local SJA for further processing requirements.

4.22.2. USDCVN Copy, Reverse: This is the area used for the probable cause statement, if necessary. The probable cause statement is a very important item on the USDCVN. Contact local SJA for guidance on completing this section.

4.22.3. After the notice is issued, the following disposition is mandatory:

4.22.3.1. The original copy (white) will be forwarded by the issuing Security Forces unit (SFAR/S-5R) to SJA who will then forward to the Central Violations Bureau.

4.22.3.2. The officer's copy (pink) will be forwarded to the Security Forces unit (SFAR/S-5R) to maintain in SFS records.

4.22.3.3. The defendant copy (yellow) and envelope is given to the violator, or if it is a parking violation, placed on the vehicle. The reverse includes instructions for the violator.

4.22.3.4. If a violation notice has been issued in error, it may only be voided for two reasons. The DFC is responsible to the United State Magistrate's Court and only voids violation notices in cases of mistaken identity of person or obvious legal error. If the agency is still in possession of all copies, the violation notice will be voided by the DFC. This ensures the integrity of the ticket issuing process. All spoiled tickets will be disposed of according to the guidelines furnished by the court.

4.22.3.5. Ensure all required information is annotated. If the violation notice has administrative errors, it will be returned to S3. If the ticket needs to be voided, the DFC must do so.

4.22.3.6. If the violation notice has already been placed on a vehicle, given to the defendant, or has been forwarded to the CVB, the notice can only be dismissed by the US magistrate judge for that district.

4.22.3.7. A written statement signed by the DFC from the agency requesting a violation notice(s) dismissal or void must be forwarded to the CVB via mail or e-mailed to the following address: [cvb@cvb.uscourts.gov](mailto:cvb@cvb.uscourts.gov).

**4.23. Federal Document-249 (FD-249)/Criminal Fingerprint Card.** DoDI 5505.11, *Fingerprint Card and Final Disposition Report Submission Requirements*, requires an FD-249, *Criminal Fingerprint Card*, be submitted on all subjects under investigation by SF for offenses listed in **Attachment 8** of the DoDI. For additional requirements and procedures for use of the Criminal Fingerprint Card, refer to AFI 31-118, Chapter 9.

**4.24. R-84/Final Disposition Report.** The R-84 must be prepared on each subject who has had an FD-249 submitted to the FBI Criminal Justice Information Services (CJIS) Division without final disposition noted. If the final disposition is not available, complete the left side and forward the form when the case is referred to the prosecutor and/or courts. If the final disposition is known when the FD-249 is submitted, it should be noted on the FD-249 which in turn makes the R-84 unnecessary. The Agency that is ultimately making the final disposition will complete and mail the R-84 to: FBI Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg WV 26306.

4.24.1. SF should fill in all arrest/apprehension data on the left side of the R-84 as the contributor of fingerprints. SF will ensure their Originating Agency Identifier (ORI) is placed in the appropriate block. If the arrest/apprehension is disposed of by SF (e.g., the offender is released without charge), SF will complete the R-84 and mail the R-84 to CJIS at the address listed in paragraph 4.20.1. In the event the case goes to the prosecutor, the R-84 should be forwarded to the prosecutor with the offender's case file. (T-0)

4.24.2. The prosecutor will complete the R-84 to show final disposition at the prosecution level is not being referred for court action and submit the R-84 to FBI/CJIS. If court action is required, the prosecutor should forward the R-84 with the case file to the court having jurisdiction. (T-0)

4.24.3. The court should complete the R-84 as to final court disposition such as when offender is acquitted, case is dismissed, conviction/sentence imposed or suspended, or person placed on probation. (T-0)

4.24.4. Completing the form. The numbers in the blocks shown on the front and reverse sides of the Form R-84 correspond to the following paragraphs describing the information you should enter into the blocks. FBI/CJIS has released several versions of the Form R-84 of which all are accepted. For the purposes of this instruction, the 2007 version was used.

**4.25. US Army Criminal Investigation Laboratory (USACIL) DNA Database Collection Card.** The collection card is contained in the collection kits provided by USACIL, as well as detailed instructions on how the kit is to be handled. All blocks on the card are to be completed in their entirety. After completion of the card, ensure the Gold Notification Card enclosed in the kit is distributed to the offender.

## Chapter 5

### SECURITY FORCES ADMINISTRATION AND REPORTS

#### 5.1. Security Forces Processing DD Form 1408, Armed Forces Traffic Ticket.

5.1.1. If the violator does not notify S5R within 5 duty days of request to rebut the citation, S5R will complete the administrative process by writing on the back of the white copy 'did not rebut' and endorse the infractions on the DD Form 1408. However, S5R must still notify the violator's first sergeant and commander of the violation. If the violator is assigned to another installation, forward the citation to the assigned installation for action. It is the responsibility of the installation to which the member is assigned to input the citation and complete the administrative action in SFMIS. (T-3)

5.1.1.1. Notification to the violator's first sergeant and commander can be accomplished either via e-mail, base information transfer system (BITS) or official mail; however, the process must be standardized and provide accountability. (T-3)

5.1.1.2. If the violator does not wish to rebut the violation, S5R inputs the citation into SFMIS; S5R will then check the appropriate response on the back of the citation and the violator requires no further action. **NOTE:** Notify the installation commander or designee for approval to revoke/suspend driving privileges for violators who have accumulated enough points. The violator's first sergeant/commander will need to escort the member to S5R for issuance of revocation/suspension letter.

5.1.2. If an individual is cited for a serious offense such as drag racing on the installation, driving while under revocation, or speeding (Art 134, Reckless Endangerment), the DD Form 1408 will be processed through S5R as outlined in paragraph 5.5., Incident Reports. The nature of these incidents may generate a report. If so, process the report and ticket together.

#### 5.2. Security Forces Processing DD Form 1408, *Armed Forces Traffic Ticket*, rebuttals.

5.2.1. If the violator wishes to make a written rebuttal, the violator must submit a rebuttal letter articulating his/her position to the DFC through S5R within 14-days of receipt of the ticket. The letter must be endorsed by his/her commander. The purpose of this endorsement is to ensure commander-level involvement. The commander must add comments supporting the violator's guilt or innocence.

5.2.1.1. S5R will obtain a written statement from the Security Forces patrolman who issued the ticket for inclusion in the rebuttal package.

5.2.2. S5R will log the DD Form 1408 into a local suspense tracking system and SFMIS and obtain the answers to the following questions to give to the rebuttal authority:

5.2.2.1. Is the offense on the citation suspendable?

5.2.2.2. If the rebuttal authority allows, does the offender wish to make a personal appearance or produce a written rebuttal?

5.2.2.3. S5R places the yellow copy of the DD Form 1408 in the suspense file pending disposition. Set 14-day suspense for command action.

5.2.2.4. Complete blocks 19-23 on the back of the white copy and annotate any prior history, points assessed and the suspense date. In the Report of Action Taken on Traffic Violation, black out the words 'No Action Taken'; this is not an option. If applicable, attach the driving history for the violator from SFMIS. Forward the white copy to the violator's commander for action. If a DD Form 1408 was issued during the course of an accident investigation, attach a copy of the accident report to the ticket when it is sent for command action.

5.2.2.5. If response on command action is not received by the due date, forward a Notice of Late Suspense memorandum, which can be electronic, providing an additional 7-day suspense. If the additional suspense is not met, send a Notice of Second Late Suspense memorandum to the unit commander with a courtesy copy to the group commander. Suspense extensions will be granted by DFCs on a case-by-case basis. Notices of Late Suspense can be completed electronically as long as S5R maintains a copy of the read receipt.

5.2.2.6. The completed package will be forwarded to the DFC for his/her annotation/recommendation and subsequently to the rebuttal authority (wing commander or designee) for final decision. Once the rebuttal authority has made a decision, S5R will notify the violator of the final outcome of his/her ticket rebuttal in writing.

5.2.2.7. Once finalized, record command action and enter it into the SFMIS case database.

### **5.3. United States District Court Violation Notice.**

5.3.1. Log the USDCVN into SFMIS. For units without SFMIS access, log the USDCVN into the local tracking system in S5R and create a file for the violator's records. Each violation requires a different USDCVN.

5.3.2. For hard copy files, file the pink copy in the suspense file pending disposition. S5R will mail the white copy to the CVB at the local Magistrate's location, unless another process has been determined by the local SJA office.

5.3.3. The CVB will set a Magistrate Court Docket list and forward it to S5R.

5.3.4. Using the CVB Docket list, pull the white and pink copies for Magistrate Court as indicated by the local staff judge advocate.

5.3.5. After the Magistrate's action, enter the actions taken in the SFMIS database.

5.3.6. Procedures for Rebutting the USDCVN:

5.3.6.1. Violators who receive a USDCVN may rebut the ticket through the Magistrate Court System on the date scheduled by the CVB. The violator may call the Magistrate for additional information regarding the status of their ticket. Staff Judge Advocate (SJA) and S5R representatives, along with the court clerk, will take into account all information presented by the violator and determine if the ticket merits dismissal. SJA has the final word on whether or not to dismiss the ticket. S5R personnel serve primarily in an advisory and administrative capacity.

5.3.6.2. If the violator still wishes to rebut the USDCVN and requests a hearing with the federal magistrate, S5R will obtain a court schedule through SJA and notify the Security

Forces patrolman who issued the citation of their scheduled appearance. The federal magistrate will make the final determination as to guilt or innocence.

5.3.6.3. CVB provides S5R with a list of the status of all processed tickets. S5R crosschecks this list with SFMIS and local ticket tracker (SFMIS applicable).

5.3.7. When your existing stock of violation notices is depleted, request form via the following website: <http://www.cvb.uscourts.gov/vn>. Enter the login name of "AGENCY" with a password of "TICKETS."

5.3.7.1. Choose the option "Request Violation Notices."

5.3.7.2. To submit a request, complete the form and click the button at the bottom of the page.

5.3.7.3. A valid CVB location code is required to order violation notices.

5.3.7.4. The CVB will send the books directly to the law enforcement agencies in the field.

#### **5.4. Processing Incident Reports.**

5.4.1. Review reports for accuracy and required information. If a report is incomplete, return it to the appropriate office with a suspense for returning the corrected report.

5.4.2. Ensure when Security Forces patrolmen enter a report into the SFMIS database that all appropriate fields are filled in without NIBRS/DIBRS errors. If a Report of Investigation (ROI) is completed by Security Forces Investigations, regardless if it is the initial report or follow-up report, ensure the entire ROI is entered into SFMIS (to include the synopsis, interviews, etc.).

5.4.3. Establish a 60-day suspense for reports requiring commander action and place them in a suspense file. Annotate the suspense date on the cover letter of the report. If prior histories exist, print and attach the history to the report for the commander's information. (**NOTE:** Prior histories are normally provided only for suspects/subjects of the report.) If response on command action is not received by the due date, forward a Notice of Late Suspense memorandum establishing an additional 14-day suspense. If the additional suspense is not met, forward a Second Notice of Late Suspense memorandum to the unit commander with a courtesy copy to the group commander. The DFC will only extend suspense dates on a case-by-case basis. Notices of Late Suspense can be completed electronically as long as S5R maintains a copy of the read receipt.

5.4.3.1. Incident reports require command action. They must be signed by the subject's unit/squadron commander. First sergeants or other personnel may complete the administrative process of the report; however, the report must be signed by the unit/squadron commander.

5.4.3.2. An e-mail with the Common Access Card (CAC) enabled digital signature can satisfy the commander's signature for closeout of the incident.

5.4.4. For reports on civilians not affiliated with the base or retired military and their family members over the age of 18, forward the report and the USDCVN(s) to the US Magistrate or local District Attorney for consideration of prosecution. If the case involves military type crimes such as driving in a restricted area, missing ID cards, etc., forward to the base

commander or designee for disposition. If the report is on a juvenile, local procedures will identify the action authority.

5.4.5. For incidents involving members from other DoD components, the initial incident report will be logged into the SFMIS database. Forward an action copy to the individual's installation provost marshal/master at arms/military police unit. Annotate forwarding of the report in the narrative portion.

5.4.6. For incident reports involving Air Force personnel away from their home station, log the report into the SFMIS database and forward an action copy to the member's home station DFC for processing. The individual's home station S5R will track the incident for final disposition/ commander's action through the SFMIS database using the existing record and case number entered by the base where the incident occurred. Do not generate a new case. Use the existing case previously entered into SFMIS.

5.4.7. Information Only reports are reports with no subject. Annotate the "Action Required" in the SFMIS database with "Information Only." Provide a copy of the report to appropriate commanders upon request or per local policy.

5.4.8. Reports sent for additional investigation:

5.4.8.1. If a report needs additional investigation by Security Forces Investigations (S2I), forward a copy of the AF Form 3545A, *Incident Report*, and all attachments (if not received from SFMIS) to S2I.

5.4.8.2. If a report is investigated by the Air Force Office of Special Investigations (AFOSI), a copy of the report with a Request for Investigation/Declination cover letter is sent with a 21-day suspense. The letter must be returned with OSI's Special Agent in Charge or designee written acceptance/declination. SFMIS will be updated to show the transfer. (T-2)

5.4.8.3. Reports are not releasable until the final investigation is completed IAW AFI 33-332 and DoDR 5400.7, *Freedom of Information Act*. Upon completion of the investigation, reports may be released to the SJA, as necessary. Unit commanders receive either an action or information copy of the report.

5.4.9. Reports Not Returned by the Suspense Date:

5.4.9.1. If response is not received by the due date, contact the investigating agency to see if the investigation is ongoing. Keep the DFC advised as to why the report has not met the suspense and have the DFC determine what action should be taken. Extensions may be granted on a case-by-case basis.

5.4.9.2. Keep all correspondence or make a memo concerning any communication about a case and file with the report.

## **5.5. Forwarding of Driving/Criminal Records/Suspension, Revocation and Debarment.**

5.5.1. Upon receipt of PCS orders or notification via Virtual Military Personnel Flight (VMPF), conduct a SFMIS check. The SFMIS feature for the forwarding of records will be utilized for PCS moves.

5.5.2. If the violator is pending commander action for a citation or criminal activity, attempt to place the violator on administrative hold until the action has been completed. If a member

refuses to give S5R any needed information, inform them they cannot be out-processed until it is provided.

5.5.3. The Commander Support Staff (CSS) must be listed on the Security Forces Squadron out-processing checklist for both PCS and TDY. Review the latest admin hold list prior to clearing a member. If there are any questions about whether or not a member can be released, consult SJA.

## **5.6. Preparation of DUI/DWI, No Proof of Insurance or Revocation/Suspension of Base Driving Privileges Packages.**

5.6.1. Prepare a folder (this can be electronic or hard copy) on the individual with the following paperwork:

5.6.1.1. Request for legal review/coordination.

5.6.1.2. Copy of the preliminary or driving revocation letter (pre-signed by the wing commander or his/her designee and normally issued by the apprehending/detaining Security Forces patrolman).

5.6.1.3. Copy of the DUI/DWI, no insurance, driving while license suspended/revoked report or ticket (to include any command action already taken).

5.6.1.4. Any blood test drug/alcohol results (if available/applicable).

5.6.2. Input revocations and suspensions information into the SFMIS database and follow routing procedures. The installation commander or designee is the final action authority for these packages.

5.6.3. Installation commanders may honor suspensions from other installations on a case-by-case basis per AFI 31-218(I), *Motor Vehicle Traffic Supervision*.

5.6.4. If a certified suspension/revocation letter is returned as undeliverable, ensure S5R retains the original with the case file and forwards a copy to the S3. If contact is made with the subject on base, Security Forces will issue the letter and forward the signed letter to S5R for attachment to the case file.

5.6.4.1. If a military member's driving privileges are suspended/revoked, then his/her unit commander or designee must be notified.

5.6.4.2. Overseas locations will develop procedures IAW host nation agreements.

5.6.5. Update the suspension/revocation/debarment listing as soon as the installation commander or designee signs the package.

5.6.6. Once the letter is returned with the appropriate signature, inform the individual's commander. The individual and their supervisor must report to S5R where the individual will sign the final revocation letter. If the person is not military affiliated, send the letter by certified mail to the violator's listed address. If overseas, local procedures will be developed to meet notification needs.

5.6.7. If a rebuttal is requested, provide the individual with instructions to submit their rebuttal letter through S5R to the installation commander (or designee) for driving revocations and the installation commander only for debarments.

**5.7. Notifying State Licensing Offices.** Notify state licensing agencies (state offense occurred in and the issuing state of driver's license), by mail, of all DUI/DWI cases as well as revocations of base driving privileges or refusal to submit to a blood alcohol test. A sample memo is located in [Attachment 3](#). Telephone numbers for state agencies are located in [Attachment 4](#). Many of these state licensing offices addresses can be found online.

**5.8. Debarment Authority.** Under the authority of 50 U.S.C. § 797 and DoDD 5200.8, *Security of DoD Installations and Resources*, installation commanders may deny access to the installation through the use of a debarment order/letter. Installation commanders may not delegate this authority. (T-0)

5.8.1. Debarment Orders. Debarment orders will be coordinated through SJA. Documentation supporting debarment must be kept for the period of the debarment. Debarment orders should be in writing and contain sufficient details to support prosecution by civilian authorities. The debarment order must also state a specific, reasonable period for the debarment. Oral debarment orders should be given only when time constraints prevent preparing a written order (letter), or the severity of the incident warrants immediate debarment. In all cases, debarment must be immediately followed-up in writing. SFMIS contains debarment information. An example is available in [Attachment 5](#).

5.8.1.1. If practical, debarment letters will be hand-delivered.

5.8.1.2. If hand delivery is impracticable, debarment letters should be sent via certified mail to ensure a record of receipt.

5.8.1.3. Debarment information will be placed into SFMIS. S5R will ensure the Site Security Manager (SSM) at their location is forwarded the most current Debarment information. This will be done every time an individual is debarred. The information will be placed in DBIDS.

5.8.2. Installation commanders may honor debarments from other installations on a case-by-case basis per Title 18 United States Code Section 1382. For further information on Debarments, refer to AFI 31-113.

## **5.9. Preparation of Revocation of Exchange/Commissary Privileges Packages.**

5.9.1. Review report and ensure an on-scene revocation of AAFES/Commissary Privileges Letter was issued. This letter is locally generated.

5.9.2. Prepare the final AAFES/Commissary Revocation Letter and a copy of the case for local SJA and installation commander or designee for signature. This process can be modified through local procedures approved by installation commander or designee and SJA. Ensure the case is updated in SFMIS accordingly. (T-3)

5.9.3. Once the letter is returned with the appropriate signature, inform the individual's commander. For military members and federal civilian employees on the installation, S5R issues the final revocation letter in person, with the individual's supervisor/sponsor present. If the person is not military affiliated, send the letter by certified mail to the violator's listed address. If overseas, local procedures will be developed to meet notification needs.

5.9.4. If using a pre-signed letter, it should be issued by the patrolman while on scene after coordination with installation commander or designee and SJA.

### 5.10. Certified Mail Procedures.

5.10.1. Use the S5R certified mail log to document certified mail. Annotate the number below the last line of the return address on the envelope. Also, put the number on the front, lower left hand corner of the Postal Service (PS) Form 3811, *Domestic Return Receipt*. If authorized, mailer may use a privately printed Form 3800, *Certified Mail Receipt*, or obtain a certified mail PS Form 3800, *Certified Mail Receipt*, and affix it to the middle, upper and front portions of the envelope. All forms should be typed. For more information refer to USPS S912.2.4 located at [www.usps.com](http://www.usps.com).

5.10.2. Prepare a Postal Service (PS) Form 3811. Annotate in section 4a the article number (the same control number listed on the PS Form 3800). In section 4b, check the box for the correspondence being sent (certified). On the bottom of the PS Form 3811, indicate the case number and/or type of incident case to which the PS Form 3811 pertains (i.e., I-00-02-050/Driving Revocation).

5.10.3. Type an AF Form 12, *Accountable Container Receipt*. In the "TO" block, type information in all capital letters: UNIT DESIGNATION, PHYSICAL ADDRESS, AIR FORCE BASE, STATE AND ZIP CODE. **NOTE:** Each envelope counts as a separate item number. Under the container number, write the S5R log number in numerical order. Under reference, write in all capital letters, CERTIFIED/RETURN RECEIPT REQUESTED for each entry. After the last entry, type dashes and the words ///LAST ITEM///. Finish the line with more dashes to the end of the row.

5.10.4. Wrap the AF Form 12 around the envelopes, which must be in numerical order, and secure them with a rubber band. When BITS picks up the mail, they will acknowledge receipt of the forms and leave the top copy of the AF Form 12 in the case folder.

5.10.5. The Postal Service will return the signed PS Form 3811 to S5R upon addressee acknowledgment. If the PS Form 3811 is returned undeliverable and is a debarment package, forward the original letters to the S3 and file the envelope along with any other receipts in the case folder. All other incidents are filed directly in the case folder.

### 5.11. Preparing Packages for Filing.

5.11.1. Once a package has been coordinated, a file folder or electronic files will be prepared with a copy of the report and signed package. Prepare the label and ensure it specifies the deletion date for the file. As a reminder, you must follow all appropriate steps before the file can be closed (i.e., driver safety course, notification to state licensing agencies, etc.). The case is then filed accordingly.

5.11.2. AFOSI is the agency responsible for putting data into the Defense Clearance Investigations Index (DCII). Security Forces will provide original reports of investigations, AF Forms 3545A, *Incident Reports*, and USDCVN to AFOSI. S5R will maintain copies of these reports IAW disposition of records requirements.

**5.12. Requests for Information.** Requests for reports will be processed IAW AFI 33-332; DoD 5400.7-R\_AFMAN 33-302, *Freedom of Information Act (FOIA) Program*; thru the S5R office only or FOIA office (follow instructions in paragraph 1.12.). The routine uses for Security Forces incident reports, including traffic violation reports, are listed in the applicable Security Forces System of Records Notice (SORN) located

at:<http://dpclo.defense.gov/Privacy/DODComponentArticleList/tabid/6799/Category/277/department-of-the-air-force.aspx>. All information released will be marked "For Official Use Only"; it is the releasers duty to ensure documents are marked correctly.

**5.13. Conducting Local Records Checks.** Law enforcement/official government agencies may request local record checks. These requests will be written, e-mailed, faxed (on official letterhead) or delivered in person with proper identification from requester. Criminal checks as part of a law enforcement investigation require no prior consent from the person(s) being checked. Only local base records checks can be conducted by S5R. Using the NCIC for employment background checks is not authorized IAW federal law, 28 U.S.C. § 534, and as discussed in the National Law Enforcement Telecommunications Systems Handbook, dated 1 Jan 99.

**5.14. Tracking Reports and Statistics.** AF Forms 53, *Security Forces Blotter*, are received by S5R via e-mail, on a unit server, and/or hard copy. S5R maintains all AF Forms 53 IAW AFI 33-364, *Records Disposition Procedures and Responsibilities*. Ensure all AF Forms 3545A, DD Forms 1408, USDCVNs and AF Forms 1315, *Major Accident Report*, are completed and/or issued into SFMIS or arrange for the responding patrolmen to input information into SFMIS. Identify all trackable incidents in the blotter and enter them into SFMIS according to category, (e.g., Larcenies, Accidents, DUIs, Suicide Attempts, Damage to Property) and for statistical crime data information reporting.

**5.15. Management and Disposition of Security Forces Files.**

5.15.1. Security Forces files will consist of reports, tickets, forms, patrolman notes, etc. **NOTE:** The installation may choose to use an electronic file plan. If used, paper records should not be destroyed until they are no longer needed for revision, dissemination, or reference, whichever is later IAW AF RDS, Table Notes 212-214.

5.15.2. Records will be recorded and maintained IAW AF RDS, Table 31-01: Security Law Enforcement Records, Table 31-102: Security Correction Records and table 31-13: Security Incident-Based reporting.

5.15.3. All information containing Privacy Act data or sensitive information will be properly disposed of as required by AFI 33-364 and AFI 33-332, will be maintained IAW AFMAN 33-363 and will be disposed of IAW the Air Force Records Disposition Schedule (RDS).

**5.16. Disposition of Files from Active to Inactive and Staging.**

5.16.1. Disposition of SFAR/S5R records is governed by AFI 33-364 and AFMAN 33-363. AF Forms 53 are destroyed (by shredding) at the end of the retention period.

**5.17. Disposition of Debarment, AAFES & Driving Revocation Packages.**

5.17.1. Remove debarment and AAFES revocation case files upon completion of the timeframe specified on the folder and put them in the inactive files to be destroyed as required by AFI 33-364.

5.17.2. Driving Revocations are removed at the end of their timeframe and put in the inactive file to be maintained IAW AFMAN 33-363 and disposed of IAW the Air Force Records Disposition Schedule (RDS).

### **5.18. Sex Offenders.**

5.18.1. The AF does not have a sex offender registry. Sex offenders living on-base must register IAW the state in which they reside. Enforcement of state laws on military installations depends upon the jurisdiction of the installation (i.e., exclusive federal, concurrent or proprietary). The real estate division of the Civil Engineer Squadron (CES) maintains records that document type of jurisdiction. In the event that jurisdiction is not clear despite CES records, installations will work with the local SJA to determine privatized housing jurisdiction. If the base has no jurisdiction, the state or county must enforce the state sex offender laws at these locations. If the on-base housing unit sits on land that is subject to exclusive or concurrent federal jurisdiction, the installation commander can enforce the state sex offender registration laws. Keep in mind that sex offender laws, such as when to register and how far the registered offender must live from a school, vary from state to state.

5.18.2. Nothing herein prevents the installation commander from debarring a sex offender from base. Such decisions must maintain good order and discipline and advance the health and welfare of the base populace, and not be arbitrary and capricious.

## Chapter 6

### LAW ENFORCEMENT INFORMATION EXCHANGE (LInX) AND DEPARTMENT OF DEFENSE LAW ENFORCEMENT DEFENSE DATA EXCHANGE (D-DEX)

**6.1. History.** LInX was developed by NCIS in 2002 and achieved Initial Operational Capability (IOC) in 2003. The concept was to provide automated and rapid sharing of law enforcement data that was already in the Records Management Systems (RMS) of the various law enforcement agencies in regions of the country of particular interest to the Department of the Navy and NCIS. The primary purposes of the system include: rapid identification of suspects, resolution of suspicious incidents, lead generation to solve crimes and prevent terrorism, “connecting the dots”, and “giving context to the dots”. The system now consists of 10 geographical regions listed below.

6.1.1. Building on the success of the LInX system, NCIS Executive Leadership determined it would be beneficial to the Department of Navy (DoN) and the Department of Defense (DoD) to develop and implement a companion system identified as the Department of Defense Law Enforcement Defense Data Exchange (D-DEX). The D-DEX system capitalizes on the LInX technology and is similar in its operation. The D-DEX system is currently operational and is connected to all 10 LInX geographical regions as well as the National Law Enforcement Data Exchange (N-DEX). Once full implementation is completed, D-DEX will contain data from the Department of Defense law enforcement agencies. The D-DEX system may contain certain information which participating DoD agencies elect not to share outside the DOD. Therefore, as described in Section 3 below, it is NCIS policy that NCIS users will only have D-DEX accounts, which permits access to both the D-DEX and LInX systems. D-DEX is a replication of an agency’s data stored on a separate and secure D-DEX server.

**6.2. Partner Systems.** LInX and D-DEX cooperate with other information sharing entities such as the National Law Enforcement Data Exchange (N-DEX) administered by the Department of Justice and various private and regional systems. In D-DEX, N-DEX can be queried from within the system by selecting the appropriate “neighborhood(s)” or it can be accessed directly through an N-DEX portal in D-DEX. Searching such partner systems is encouraged as they cover parts of the USA that are not in the LInX Regions. Users should realize that displays of data from other systems may have different data sets available and they may display differently than data from LInX agencies.

6.2.1. Information Sharing Memorandums of Agreement (MOA)/Understanding With Jurisdictions Not Participating or Covered by CJI Sharing Through N-DEX. To ensure against information sharing gaps in N-DEX, Defense Force Commanders (DFC) are authorized and encouraged to seek MOA/MOU CJI sharing agreements with allied and partner agencies (i.e. State/local LE/Police Departments (PD) not tied into N-DEX. These MOA/MOUs should contain clearly established standard operating procedures regarding scope and timeliness on how and what information will be shared. (T-3)

### **6.3. Access to Information Sharing Systems.**

6.3.1. Access to D-DEX. As previously mentioned, Security Forces users will obtain D-DEX accounts to achieve maximum benefit from the systems. D-DEX users have full access to LInX information and therefore do not require LInX accounts. AFSFC and MAJCOMs will

have a D-DEx System Administrator assigned and that person should be contacted for new accounts and training.

6.3.1.1. Initial training and an agreement to use the system only for lawful purposes are required before accessing the system. All personnel will be required to fill out a DD Form 2875 and complete current training for PII. There are various features allowing for automated system administration, self-service password help and additional video training modules. D-DEx is currently Common Access Card (CAC) enabled and will eventually be CAC enforced. Certain types of DoD users may have access limited to their need to know as listed below. (T-0)

6.3.1.1.1. Tactical User - Able to query "pointer" data only (Title, CCN and Agency/POC).

6.3.1.1.2. Analytical User - Able to query full reports. Envisioned for Special Agents, Criminal Analysts, Dispatchers and Police Watch Commanders.

6.3.1.1.3. Systems Administrator - Able to create accounts, disable accounts and block reports.

6.3.1.2. All prospective D-DEx users are required to complete a basic training course prior to accessing the data in the system. (T-0)

**6.4. Training and Certifications.** All prospective D-DEx users are required to complete a basic training course prior to accessing data in the system. Normally, D-DEx System Administrators are responsible for providing this training although they may also certify others as D-DEx Trainers who have completed the required training and exhibit the ability to train on the system. It is the responsibility of AFSFC and MAJCOMs to assist the System Administrators by providing logistical support such as arranging training spaces and managing participation. (T-0)

6.4.1. D-DEx users are encouraged to periodically review the on-line training modules and "New Features" descriptions available from the D-DEx homepage located on SMARTNet.

**6.5. Expectation of Use.** It is NCIS policy that D-DEx is expected to be used to thoroughly research relevant information on all NCIS investigations and operations regardless of category. The best practice is for the D-DEx inquiry to be conducted by the case agent, who by definition is most familiar with the case and therefore most likely to identify pertinent results. It is also permissible for D-DEx inquiries to be conducted by support personnel, assigned analysts and on urgent cases when normal D-DEx access is not available, by watch standers in the NCISHQ MTAC. In addition to the initial D-DEx inquiry normally conducted at the time the investigation is opened, periodic D-DEx inquiries should be conducted during the pendency of the case as additional information is developed. Remember, in addition to investigative support, D-DEx is a primary tool for safety. Security Forces users are encouraged to use the "watch list" function in D-DEx on active subjects so that the investigators will be alerted if the subject has a new contact with law enforcement. This function is managed under the "My D-DEx" section of the home page.

**6.6. Validation.** Data derived from D-DEx/LInX may be used for the primary purposes of rapid identification of suspects, resolution of suspicious incidents and lead generation to solve crimes without further authorization. The use of NCIS data in D-DEx by Security Forces users is

permissible in all ways that the same information is used now without further authorization. However, all D-DEX information derived from other agencies, including any analytical products derived from it, may not be used as a basis for action nor be disseminated outside of the D-DEX program for any purpose or in any other manner, unless the person making the inquiry first obtains the express permission of the agency or agencies that contributed the information in question. Included within the prohibition are any specific inclusion of D-DEX/LInX information in an official case file, and any use of such information in the preparation of judicial process such as affidavits, warrants or subpoenas without prior permission of the contributing agency. Normally, the person making the D-DEX inquiry will simply contact the contributing agency to determine if the information is current, correct and complete and to request a copy of their report for inclusion in the case file. The various Memoranda of Understanding governing D-DEX do allow for immediate use of some information under conditions of extreme danger, but follow-up with the originating agency must be made as soon as possible.

**6.7. Justification.** All D-DEX users are required to provide a reason for the inquiry in the “justification” block of the search page. In many cases, the case control number (CCN) may be used; however, a CCN is not necessary and it is adequate to include sufficient information to remind the user why he/she made the inquiry if questioned in the future such as during the audit process. Such reasons as “investigation” are not specific enough to meet the justification requirement. Some examples of proper justifications are: “ID possible theft suspect”, “locate witness”, “Get XYZ PD report number” and “verify suspect’s address”. “Testing”, “Training”, and “Demonstration” are also valid justifications for those functions. Users are generally cautioned against running themselves or acquaintances to avoid impropriety or the appearance of impropriety.

**6.8. Background Investigations.** D-DEX/LInX policy prohibits the use of these systems for employment background investigations with the exception of backgrounds conducted on prospective employees of one’s own agency. In other words, D-DEX inquiries can be run during investigations on Security Forces employees or prospective employees. It generally may not be run for other purposes such as general licensing, eligibility for federal or state benefits or background investigations for other agencies. This prohibition does not apply to background type inquiries conducted as part of any criminal or CI/CT investigation. If unique circumstances exist, contact a D-DEX Division Representative for additional information.

**6.9. Reporting Results.** When D-DEX/LInX/N-DEX information is summarized or otherwise documented, the user shall indicate that the information was obtained from the contributing agency and not D-DEX/LInX/N-DEX. A user may put very general comments on D-DEX/LInX/N-DEX in Security Forces’ reports. For example, a Security Forces ROI (OPEN) may contain this or similar language: “Reporting Investigator queried the D-DEX/LInX/N-DEX systems, which showed that Subject was identified as being a victim of a burglary investigated by XYZ Police Department in 2006 under report #123456. LInX records also indicated Subject was arrested for DUI by XYY PD in 2007 under citation #34567 and FBI #XX34561. The official records of these incidents will be requested from XYZ and XYY Police Departments. No official action will be taken without the official documents or communications with the originating agency”. The actual reports of the burglary and DUI should be sought from the police department, if relevant, and permission should be requested to include the actual report or a summary of it per current policy. (T-0)

**6.10. Printing.** The decision to temporarily print inquiry results in the LInX program is made by the regional Board of Governance or N-DEX. These governing bodies generally permit the temporary printing and retention of the copy for a period not to exceed 72 hours. These regional LInX rules are incorporated in the LInX operating system, which **prevents printing** if printing is not authorized from a particular region represented in the result set. Each printed document contains a caveat showing who printed the material and when it must be destroyed. Within the D-DEX program, temporary printing of any information has been authorized following the same 72-hour retention period. Printed D-DEX/LInX results are not to be filed in case files. System Administrators will monitor compliance through the case review and audit processes.

**6.11. Use of Photographs.** Most LInX regions and D-DEX permit the printing of photographs (mug shots) obtained from the system. The retention of these photographs follows the same 72-hour restriction unless they are used in a photographic line-up. In that case, the contributing agency should be contacted to validate the photograph and the photograph handled as per current policy.

**6.12. Sanctions.** Unauthorized use, which includes requests, dissemination, sharing, copying or receipt of D-DEX/LInX information, could result in civil proceedings against the USAF Security Forces and/or criminal proceedings against any user or other person involved. All violations should be reported to the NCIS LInX/D-DEX Division. (T-0)

6.12.1. Audits of Security Forces use of the D-DEX system will be conducted at least once per year. These audits consist of a sampling of the users and of particular individual users as warranted. The system allows for precise auditing by username, date and time. **NOTE: Administrators should audit 25% of their personnel quarterly. This process will make it easier for annual audits.** Questionable transactions will be researched and provided to the appropriate oversight entity only when necessary. It is the intent of the audit to maintain system integrity and not to discourage creative, appropriate uses of the system. Users will be presumed to be using the system for appropriate purposes and within the spirit of innovative police work and cooperation unless evidence suggests otherwise. (T-0)

6.12.2. Information Sharing Memorandums of Agreements/Understanding (MOA/MOU) with jurisdictions not participating or covered by CJIS sharing through N-DEX. To ensure against information sharing gaps in N-DEX, Defense Force Commanders (DFC) are authorized and encouraged to seek MOA/MOU CJIS sharing agreements with state and local LE Police Departments (PD) not tied into N-DEX. These MOA/MOUs should contain clearly established standard operating procedures regarding scope and timeliness on how and what information will be shared.

JUDITH A. FEDDER, Lieutenant General, USAF  
DCS/Logistics, Installations & Mission Support

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

*References*

- AFMAN 31-116, *Air Force Motor Vehicle Traffic Supervision*, 9 May 2012
- AFMAN 33-363, *Management of Records*, 1 March 2008
- AFI 31-101, *Integrated Defense*, Incorporating Change 2, 6 March 2013
- AFI 31-113, *Installation Perimeter Access Control*, 26 January 2012
- AFI 31-118, *Security Forces Standards and Procedures*, 5 March 2014
- AFI 31-206, *Security Forces Investigations*, 16 September 2009 (pending approval and publication, will become AFI 31-115, *Security Forces Investigations*)
- AFI 31-218, *Motor Vehicle Traffic Supervision*, 22 May 2006
- AFI 31-501, *Personnel Security*, 27 January 2005
- AFI 33-200, *Information Assurance (IA) Management*, Incorporating Through Change 2, 15 October 2010
- AFI 33-321, *Authentication of Air Force Records*, 3 August 2011
- AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 5 June 2013
- AFI 33-360, *Publications and Forms Management* 25 September 2013
- AFI 33-364, *Records Disposition Procedures and Responsibilities*, 22 December 2006
- AFPD 31-1, *Integrated Defense*, 28 October 2011
- AFTTP 3-31.1, *Entry Control*, 29 May 2007
- DoD 7730.47-M, Vol 1, *Manual for Defense Incident-Based Reporting System (DIBRS): Data Segments and Elements*, 7 December 2010
- DoD 7730.47-M, Vol 2, *Manual for Defense Incident-Based Reporting System (DIBRS): Supporting Codes*, 7 December 2010
- DoDD 5400.7, *DoD Freedom of Information Act Program*, 2 January 2008; Incorporating Change 1, 28 July 2011
- DoD 5400.7-R\_AFMAN 33-302, *Freedom of Information Act (FOIA)*, 21 October 2010; Incorporating Change 1, 24 April 2012
- DoDD 5525.4, *Enforcement of the State Traffic Laws on DoD Installations*, 2 November 1981; Incorporating Change 1, 31 Oct 1986
- DoDD 7730.47, *Defense Incident-Based Reporting System (DIBRS)*, 15 October 1996
- DoDI 5505.07, *Titling and Indexing Subjects of Criminal Investigations in the Department of Defense*, 27 January 2012
- DoDI 5200.8, *Security of DoD Installations and Resources and the DoD Physical Security*

*Review Board (PSRB); Incorporating Change 1, 19 May 2010*

DoDI 5505.11, *Fingerprint Card and Final Disposition Report Submission Requirements*, 9 July 2010; Incorporating Change 3 May 2011

DoDI 5505.17, *Collection, Maintenance, Use, and Dissemination of Personally Identifiable Information and Law Enforcement Information by DoD Law Enforcement Activities*, 19 December 2012

DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007

DoDD 8570.1, *Information Assurance (IA) Training, Certification and Workforce Management*, 15 August 2004

DTM-09-012, *Interim Policy Guidance for DoD Physical Access Control*, 8 December 2009

Title 50 United States Code Section 797; Incorporating Change, 9 September 2012

Air Force Records Information Management System (AFRIMS)

Lautenberg Amendment, *Firearms Prohibition and Domestic Violence Convictions*, amendment to the *Gun Control Act of 1968*

Section 534, United States Code, *Uniform Federal Crime Reporting Act*, January 2004

Sections 10606 and 10607 of Title 42, United States Code, *Victims Rights and Restitution Act of 1990*, January 2004

Section 922 of Title 18, United States Code, *The Brady Handgun Violence Prevention Act 2008*

System of Records Notices (SORN) F031 AF SF B, *Security Forces Management Information System (SFMIS)*, March 18, 2010; F031 AF SP F, *Notification Letters to Persons Barred from Entry to Air Force Installations*, August 7, 2009; and F031 AF SP O, *Documentation for Identification and Entry Authority*, 11 June 1997

## **Forms**

### **Adopted Forms:**

AF Form 12, *Accountable Container Receipt*

AF Form 52, *Evidence Tag*, 1 July 1986

AF Form 53, *Security Forces Desk Blotter*, 1 December 2000

AF Form 75, *Visitor/Vehicle Pass*, 1 June 2002

AF Form 522, *USAF Ground Weapons Training Data*, 1 July 1999

AF Form 623a, *On the Job Training Record-Continuation Sheet*, 1 March 1979

AF Form 847, *Recommendation for Change of Publication*, 22 September 2009

AF Form 1109, *Visitor Register Log*, 1 May 1999

AF Form 1168, *Statement of Suspect/Witness/Complainant*, 1 April 1998

AF Form 1176, *Authority to Search and Seize*, 28 March 2003

AF Form 1199 Series, *USAF Restricted Area Badges*, 1 November 1986  
AF Form 1313, *Driver Record*, 1 May 1985  
AF Form 1315, *Accident Report*, 1 July 1994  
AF Form 1361, *Pick-Up/Restriction Order*, 28 March 2003  
AF Form 1364, *Consent for Search and Seizure*, 1 September 2001  
AF Form 2586, *Unescorted Entry Authorization Certificate*, 1 October 1998  
AF Form 3226, *Authority to Apprehend in Private Dwelling – Resident*, 1 January 1994  
AF Form 3545, *Incident Report*, 11 May 2005  
AF Form 3907, *Security Forces Field Interview Data*, 1 September 2001  
AF Form 4443, *Law Enforcement and Physical Security Activities Report (LEPSAR)*, 1 April 2015  
DD Form 460, *Provisional Pass*, March 1951  
DD Form 1131, *Cash Collection Voucher*, December 2003  
DD Form 1408, *Armed Forces Traffic Ticket*, December 1987  
DD Form 1920, *Alcoholic Incident Report*, November 2004  
DD Form 2701, *Initial Information for Victims and Witnesses of Crime*, May 2004  
DD Form 2708, *Receipt for Inmate or Detained Person*, November 1999  
DD Form 2875, *System Authorization Access Request (SAAR)*, August 2009  
Federal Document-249 (FD-249), *Criminal Fingerprint Card R-84, Final Disposition Report*, 11 May 1999  
R-841 Final Disposition Report  
Postal Service (PS) Form 3811, *Domestic Return Receipt*  
PS Form 3800, *Certified Mail Receipt*  
PS Form 3811, *Domestic Return Receipt*  
Standard Form 135, *Records Transmittal and Receipt*  
United States District Court Violation Notice

### ***Abbreviations and Acronyms***

**ACP**—Access Control Point

**AD**—Active Duty

**AAFES**—Army and Air Force Exchange Service

**AF**—Air Force

**AFB**—Air Force Base

**AFPEO EIS**—Air Force Program Executive Office Enterprise Information Systems

**AFI**—Air Force Instruction  
**AFMAN**—Air Force Manual  
**ANG**—Air National Guard  
**AFOSI**—Air Force Office of Special Investigations  
**AFRIMS**—Air Force Records Information Management System  
**AFSC**—Air Force Specialty Code  
**AFSFC**—Air Force Security Forces Center  
**AFTR**—Air Force Training Record  
**AFVA**—Air Force Visual Aid  
**AKA**—Also Known As  
**AT/FP**—Antiterrorism/Force Protection  
**AWOL**—Absent Without Leave  
**B&E**—Breaking and Entering  
**BAC**—Blood Alcohol Content  
**BEQ**—Bachelor Enlisted Quarters  
**BDOC**—Base Defense Operations Center  
**BITS**—Base Information Transfer System  
**BOLO**—Be On the Look Out  
**BSO**—Base Security Officer  
**BX**—Base Exchange  
**CAC**—Common Access Card  
**CBT**—Computer Based Training  
**CC**—Commander  
**CCB**—Configuration Control Board  
**CCH**—Computerized Criminal History  
**COCO**—Contractor-owned, contractor-operated  
**CONUS**—Continental United States  
**COP**— Common Operating Picture  
**CSS**—Commander Support Staff  
**CVB**—Central Violations Bureau  
**DAA**—Designated Accrediting Authority  
**DAC**—DBIDS Access Card

**DAF**—Department of the Air Force  
**DBIDS**—Defense Biometric Identification System  
**DCII**—Defense Clearance Identification Index  
**DEROS**—Date Eligible for Return from Overseas  
**DFC**—Defense Force Commander  
**DIACAP**—Department of Defense Information Assurance Certification & Accreditation Process  
**DIBRS**—Defense Incident-Based Reporting System  
**DMDC**—Defense Manpower Data Center  
**DoD**—Department of Defense  
**DoDD**—DoD Directive  
**DoDI**—DoD Instruction  
**DoDID**—DoD Identification  
**DoDR**—DoD Regulation  
**DSN**—Defense Switch Network  
**DUI**—Driving Under the Influence  
**DWI**—Driving While Intoxicated  
**ECC**—Emergency Control Center  
**EIRE**—Erroneous Incident Report Entries  
**FARM**—Functional Area Records Manager  
**FAS**—Field Assistance Service  
**FBI**—Federal Bureau of Investigations  
**FD**—Federal Document  
**FOIA**—Freedom of Information Act  
**FOUO**—For Official Use Only  
**FPCON**—Force Protection Condition  
**FRB**—Functional Review Board  
**FSA**—Functional System Administrator  
**GIG**—Global Information Grid  
**GOCO**—Government-owned, contractor-operated  
**GOV**—Government Owned Vehicle  
**HQ**—Headquarters  
**HQ AFOSI**—HQ Air Force Office of Special Investigations

**IACS**—Installation Access Control System  
**IAM**—Information Assurance Manager  
**IAW**—In Accordance With  
**ID**—Identification  
**IDRMP**—Integrated Defense Risk Management Process  
**III**—Interstate Identification Index  
**IS**—Information System  
**LAN**—Local Area Network  
**LEO**—Law Enforcement Officer  
**MAJCOM**—Major Command  
**MCM**—Manual for Courts Martial  
**MICT**—Management Internal Control Toolset  
**NCIC**—National Crime Information Center  
**NCO**—Noncommissioned Officer  
**NIBRS**—National Incident-Based Reporting System  
**NLETS**—National Law Enforcement Terminal System  
**OAC**—Originating Agency Case  
**OCA**—Arrest Number  
**OCONUS**—Outside of Continental United States  
**OI**—Operating Instruction  
**OUSD (P & R)**—Office of the Under Secretary of Defense for Personnel and Readiness  
**OPR**—Office of Primary Responsibility  
**PACS**—Physical Access Control System  
**PCCIE**—Power Conditioning and Continuation Interfacing Equipment  
**PCS**—Permanent Change of Station  
**PD**—Property Damage  
**PI**—Personal Injury  
**PII**—Personal Identification Information  
**PIV**—Personal Identity Verification  
**POV**—Privately Owned Vehicle  
**POW**—Privately Owned Weapon  
**PS**—Postal Service

**PWS**—Performance Work Statement  
**RAB**—Restricted Area Badge  
**RAM**—Random Antiterrorism Measure  
**RDS**—Record Disposition Schedule  
**ROI**—Report of Investigation  
**ROS**—Report of Survey  
**S2I**—Security Forces Investigations  
**S3**—Security Forces Operations Branch  
**S5R**—Security Forces Administration and Reports  
**SF**—Security Forces  
**SFAR**—Security Forces Administration and Reports/S5R  
**SFMIS**—Security Forces Management Information System  
**SFOP**—Security Forces Operations Police  
**SFST**—Standardized Field Sobriety Test  
**SFX**—Security Forces Requirements  
**SID**—State Bureau Number  
**SJA**—Staff Judge Advocate  
**SOC**—Social Security Number  
**SRB**—Suspension/Revocation/Debarment  
**SSL**—Secured Socket Layer  
**SSM**—Site Security Manager  
**SSN**—Social Security Number  
**STS**—State Terminal System  
**TAC**—Terminal Agency Coordinator  
**TDY**—Temporary Duty  
**TSC**—Terrorist Screening Center  
**UCMJ**—Uniform Code of Military Justice  
**US**—United States  
**USAF**—United States Air Force  
**U.S.C.**—United States Code  
**USDCVN**—United States District Court Violation Notice  
**UTA**—Unit Training Assembly

**VCC**—Visitor Control Center

**VWAP**—Victim/Witness Assistance Program

**VMPF**—Virtual Military Personnel Flight

**WDMS**—Working Dog Management System

**WMS**—Warehouse Management System

**WWW**—World Wide Web

**ZIP**—Zone Improvement Plan

**Attachment 2**  
**SAMPLE MEMO**

**Figure A2.1. Sample Memo.**

<p>MEMORANDUM FOR DEPARTMENT OF VEHICLE REGISTRATION AND LICENSES  Street Address  City, State Zip Code</p> <p>FROM: XX Security Forces Squadron  Street Address  City, State Zip Code</p> <p>SUBJECT: Notification of Person Convicted of an Intoxicated Driving Offense</p> <p>1. This memo is to notify you that on (date), (last name, first name, middle initial) (social security number of person), a member of the (branch of Military Service or DoD Component), (unit), (installation location), was found guilty of (intoxicated driving or refusal to take a blood alcohol content (BAC) test in a court-martial, non-judicial proceeding under Article 15 of the UCMJ or civil court). (If civil court, give court name and case number). (He/she) holds a (state) driver's license, number (put in number), issued (issuing date), expiring on (expiration date). (He/she) was apprehended by (name of SF member or police officer) on (date and location) while driving vehicle license number (put in vehicle information).</p> <p>2. A BAC (was or was not) taken with a reading of (include BAC results, if available). Based upon the above information, this individual's installation driving privileges have been (<u>suspended/revoked</u> for) (insert number of years). The individual's current address is: (put in individual's address).</p> <p style="text-align: center;">SIGNATURE BLOCK OF SFAR/S5R</p> <p>PROTECTED BY THE PRIVACY ACT OF 1974 – this communication contains personal information which must be protected IAW DoD5400.11R and is FOR OFFICIAL USE ONLY.</p>
--

**Attachment 3****TELEPHONE NUMBERS/ADDRESSES FOR STATE AGENCIES NOTE**

This list contains each state's licensing agency information. However, it is recommended that prior to mailing any documentation to one of the below addresses, first verify the relevancy of the address in the event it has changed.

Alabama: Motor Vehicle Division, P.O. Box 327630, Montgomery AL 36132-7630, (334) 242-9000.

Alaska: Division of Motor Vehicles, 1300 W. Benson Blvd Ste 900, Anchorage AK 99503-3696, (907) 269-3750.

Arizona: Motor Vehicle Division, PO Box 2100, Phoenix AZ 85001-2100, (602) 255-0072.

Arkansas: Motor Vehicle Division, 1900 W. 7th Street #1040, Little Rock AR 72201, (501) 682-4630.

California: Department of Motor Vehicles, P.O. Box 932340, Sacramento CA 95814, (916) 229-0370.

Colorado: Motor Vehicle Division, 1935 W. Mississippi Avenue, Denver CO 80223, (303) 937-9507.

Connecticut: Department of Motor Vehicles, 60 State Street, Wethersfield CT 06109, (860) 263-5700.

Delaware: Motor Vehicle Director, 800 Bay Road, Dover DE 19901, (302) 378-8930.

District of Columbia: Department of Transportation, Bureau of Motor Vehicles, 1205 Brentwood Road Northeast, Washington DC 20018, (202) 727-5000.

Florida: Division of Motor Vehicles, 2900 Apalachee Parkway Rm B 435, Tallahassee FL 32399, (850) 617-2600.

Georgia: Motor Vehicle Division, 6840 West Church Street, Atlanta GA 30303, (770) 920-3918.

Hawaii: Division of Motor Vehicle and Licensing, 1455 S. Beretania Street, Honolulu HI 96814, (808) 527-6695.

Idaho: Transportation Department, P.O. Box 7129, Boise ID 83707-1129, (208) 334-8735.

Illinois: Secretary of State, 107 W. Cook Street #B, Springfield IL 62704, (217) 753-2323.

Indiana: Bureau of Motor Vehicles, 4050 Meadows Parkway, Indianapolis IN 46205, (317) 547-3572.

Iowa: Department of Transportation Office of Operating Authority, P.O. Box 9204, Des Moines IA 50306, (515) 244-9124.

Kansas: Driver's Licensing, Docking Station Office Bldg., P.O. Box 2188, Topeka KS 66601-2128, (785) 296-3963.

Kentucky: Department of Transportation, 101 Cold Harbor Drive, Frankfort KY 40601, (502) 564-6800.

Louisiana: Motor Vehicle Administrator, 7979 Independence Blvd., Baton Rouge LA 70806, (225) 922-1175.

Maine: Department of State, Motor Vehicle Division, 19 Anthony Ave., Augusta ME 04330, (207) 287-3330.

Maryland: Motor Vehicle Administration, 6601 Ritchie Highway, NE, Glen Burnie MD 21062, (301) 729-4550.

Massachusetts: Drivers Control Suspension Certified, P.O. Box 55896, Boston MA 02205-5896, (617) 351-4500.

Michigan: Department of State, Division of Driver Licenses and Vehicle Records, Lansing MI 48918, (888) 767-6424.

Minnesota: Department of Public Safety, 1472 University Ave., St. Paul MN 55104, (651) 297-3298.

Mississippi: Department of Motor Vehicles, P.O. Box 1033, Jackson MS 39215-1033, (601) 923-7000.

Missouri: Department of Revenue, Motor Vehicles Bureau, Harry S. Truman Bldg., 301 W. High Street, Jefferson City MO 65105, (573) 751-4509.

Montana: Motor Vehicle Division, Scott Hart Bldg., 2d Floor, 303 North Roberts, P.O. Box 201430, Helena MT 59620-1430, (406) 444-1772.

Nebraska: Driver's Licensing Services, 301 Centennial Mall South, P.O. Box 94726, Lincoln NE 68509-4726, (402) 471-3861.

Nevada: Department of Motor Vehicles, 555 Wright Way, Carson City NV 89711, (775) 684-4368.

New Hampshire: Department of Safety, Division of Motor Vehicles, James H. Haynes Bldg., 23 Hazen Drive, Concord NH 03305-0002, (603) 271-2371.

New Jersey: Motor Vehicle Division, P.O. Box 403, Trenton NJ 08666-0403, (609) 292-6500.

New Mexico: Motor Transportation Division, Joseph M. Montoya Building, Santa Fe NM 87504-1028, (888) 683-4636.

New York: Division of Motor Vehicles, Swan State Building, Empire State Plaza, Albany NY 12228, (518) 473-5595.

North Carolina: Division of Motor Vehicles, Motor Vehicles Bldg., 1100 New Bern Ave., Raleigh NC 27697, (919) 715-7000.

North Dakota: Motor Vehicle Department, 608 East Boulevard Ave., Bismarck ND 58505-0700, (701) 328-2500.

Ohio: Bureau of Motor Vehicles, P.O. Box 16520, Columbus OH 43216-6520, (614) 752-7500.

Oklahoma: Oklahoma Tax Commission, Motor Vehicle Division, 3600 North Martin Luther King Blvd., Oklahoma City OK 73111, (405) 681-5489 .

Oregon: Motor Vehicles Division, 1905 Lana Avenue, NE, Salem OR 97314, (503) 945-5000.

Pennsylvania: Department of Transportation, Bureau of Motor Vehicles, 1011 South Front Street, Harrisburg PA 17104, (717) 412-5300.

Rhode Island: Department of Motor Vehicles, 100 Main Street, Pawtucket RI 02903, (401) 462-4368.

South Carolina: Motor Vehicle Division, P.O. Drawer 1498, Bythewood SC 29016, (803)896-5000.

South Dakota: Division of Motor Vehicles, 445 East Capitol, Pierre SD 57501, (605) 773-2550.

Tennessee: Department of Revenue, Motor Vehicle Division, P.O. Box 945, Nashville TN 37202, (615) 253-5221.

Texas: Department of Highways and Public Transportation, Motor Vehicle Division, 5805 North Lamar Blvd, Austin TX 78773-0001, (512) 424-2000.

Utah: Motor Vehicle Division, 210 North 1950 West, Salt Lake City UT 84134, (800) 368-8824.

Vermont: Department of Motor Vehicles, 120 State Street, Montpelier VT 05603, (802) 828-2085.

Virginia: Department of Motor Vehicles, P.O. Box 27412, Richmond VA 23269, (800) 435-5137.

Washington: Department of Licensing, P.O. Box 9030, Olympia WA 98507, (360) 902-3900.

West Virginia: Department of Motor Vehicles, Bldg. 3 Room 138, Charleston WV 25317, (304) 558-3900.

Wisconsin: Department of Transportation Reciprocity and Permits, 2001 Bartillon Dr., Madison WI 53704, (608) 266-2353.

Wyoming: Department of Revenue, Policy Division, 5300 Bishop Blvd., Cheyenne WY 82009, (307) 777-4803.

Guam: Deputy Director, Revenue and Taxation, Government of Guam, Agana, Guam 96910, (671) 635-7652.

Puerto Rico: Department of Transportation and Public Works, Bureau of Motor Vehicles, P.O. Box 41243, Minillas Station, Santurce, Puerto Rico 00940, (809) 722-2823.

## Attachment 4

## SAMPLE FORMAT FOR A DEBARMENT LETTER

Figure A4.1. Sample Format for a Debarment Letter.

**(Use Appropriate Letterhead)**

MEMORANDUM FOR

FROM:

SUBJECT: Order Not To Enter or Reenter (Installation Name)

1. It has come to my attention that you [describe incident(s) in detail; for example, "were found in possession of marijuana at the on-base quarters of Staff Sergeant John Smith on 15 January 2008."].
2. Based upon the above, I consider your continued presence on this installation to be detrimental to the maintenance of good order and discipline. Effective immediately, you are ordered to not enter or reenter (installation name) for a period of (state the time frame).
3. If you fail to comply with this order, you will be subject to prosecution under Title 18 United States Code §1382, which reads in part:  
  
"Whoever reenters or is found within any installation, after having been removed there from or ordered not to reenter by any officer or person in command or charge therefore shall be fined under this title or imprisoned not more than six months, or both."
4. Should you reenter (installation name) in violation of this order, without having received prior approval, you will be subject to detention by the Security Forces for delivery to the appropriate civilian and military authorities.
5. If you are entitled to medical treatment at (hospital name), you may enter (installation name) for the sole purpose of using said facility. To do so, you must present this letter to the entry controller at the installation entry point and obtain the appropriate visitor pass. You will travel directly to the medical facility by [describe precise route the individual must travel to go to and from the medical facility]. You may not deviate from this route nor stop for any reason on your way to or from the facility.
6. Under extraordinary circumstances, requests for temporary access to other facilities on (installation name) may be granted. Such requests should be made in advance and in writing through the Chief of Security Forces, and set out the reason(s) why access should be granted. If time does not permit, such a request must be made to the Security Forces control center at (phone number). The controller will then notify the appropriate officials and convey your request.
7. This order will remain in effect [(indefinitely) or (for the period prescribed above)], unless otherwise modified or revoked in writing by myself. If a compelling reason exists which you believe should be sufficient to justify modification or termination of this order, you may submit your justification to me, in writing, through the Chief of Security Forces.

Installation Commander's Signature Block

cc:

SFS Reports and Analysis Branch

1st Ind, (name of first indorser)

MEMORANDUM FOR (installation commander office symbol)

This is to certify that I, the undersigned, have received the forgoing order in writing and have read and fully understand the same. I understand that entry upon (installation name), in violation of this order, may result in civilian prosecution pursuant to Title 18 U.S.C. §1382. I further understand that in the event of a conviction, the maximum penalty prescribed may be imposed.

Received and signed the \_\_\_\_\_ day of \_\_\_\_\_, 20 \_\_\_\_.

Signature Block and/or Signature of Debarred Individual

2d Ind, (office symbol of 2d indorser)

MEMORANDUM FOR (installation commander office symbol)

**CERTIFICATION**

This is to certify that I (Patrolman's name) \_\_\_\_\_, personally served a copy of the debarment letter to (Debarred individual) \_\_\_\_\_, on \_\_\_\_\_ ( date).

Signature Block of Issuing Security Forces Member