BY ORDER OF THE COMMANDER
AIR FORCE SUSTAINMENT CENTER

AIR FORCE SUSTAINMENT CENTER
INSTRUCTION 33-101

12 DECEMBER 2014
Incorporating Change 1, 3 NOVEMBER 2015

Communications and Information

PROVISIONING/DEPROVISIONING OF AFSC MANAGED INFORMATION SYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: AFSC/LGMS

Certified by: AFSC/LGA
(Steven L. Cain)
Pages: 7

This publication defines the standard repeatable process the Air Force Sustainment Center (AFSC) will use to provision and deprovision from AFSC managed information systems using DD Form 2875 System Authorization Access Request (SAAR). This instruction applies to all military, contractors and civilian and members using or managing AFSC managed information systems. Refer recommended changes and questions about this publication to the OPR listed above using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate chain of command to AFSC/LGM. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS).

SUMMARY OF CHANGES

This interim change revises AFSC 33-101 by: (1) **Changing: Information Owner/OPR (AKA the Functional Advocate).** Manages HQ AFMC or AFSC Center-level policy, business processes, and functional systems requirements for a specific IS to **Information Owner.** Manages AFSC Center-level policy, business processes, and functional systems requirements for a specific information system and responsible for approving access to this information system.

(2) Changing: The Supervisor will sign the DD Form 2875 request and it is then sent to the Organization Security Manager/Monitor to Once approved, the Supervisor will sign the DD Form 2875 request (blk #18) and it is then sent to the Organization Security Manager/Monitor. (3) Changing: **User will:** Forward the completed request to the Organization IAO or Appointee to **User will:** Forward the completed DD Form 2875 request to the System IAO or appointed system access authority. If the System IAO is unknown, the User will contact the system's Information Owner (Note: For some systems, the AF Portal Applications A-Z can be used to find the Information System POC). (4) Changing: **Organization IAO or Appointee will:** Accept the DD Form 2875 request and verify it is approved and signed by the User, Supervisor, and Organization Security Manager. The Organization IAO or Appointee will then validate the DoD Information Assurance CyberAwareness Challenge (blk #10) is current and the User has signed (blk #11). The Organization IAO or Appointee will sign the DD Form 2875 request (blk# 22) and send the form back to the User to **System IAO or Appointed System Access Authority will:** Accept and review the DD Form 2875 request to ensure the User meets the security requirements for the information system. Once approved, sign the DD Form 2875 request (blk #22). The System IAO or appointed system access authority will then send the DD Form 2875 request to the Information Owner. (5) Changing: **Information Owner will:** Review the DD Form 2875 request for completeness and specifically ensure the User is authorized to have access based on the User's justification stating his/her duties as it relates to requesting access to the information system. Once reviewed, the Information Owner will sign the DD Form 2875 request (blk # 21) and send it to the System IAO to **Information Owner or office designated by the Information Owner will:** Review the DD Form 2875 request for completeness and specifically ensure the User is authorized to have access based on the User's justification stating his/her duties as it relates to requesting access to the information system. Once approved, the Information Owner or office designated by the Information Owner will sign the DD Form 2875 request (blk # 21) and then request system access to the organization granting access (i.e. DISA). (6) Changing: **User will**: Send an e-mail to the Information Owner to request deprovisioning from the system; if the POC is unknown, go to the AF Portal Applications A-Z to find the POC. Note: in some cases, the e-mail will be sent to the Program Management Office (PMO) to **User will**: Send an e-mail to the Information Owner or office designated by the Information Owner to request deprovisioning from the system. (7) Changing: **Information Owner (or PMO) will:** Request to deprovision the User and send a confirmation e-mail to the User stating that the User is or will be deprovisioned to **Information Owner or office designated by the Information Owner will:** Request to deprovision the User and send a confirmation e-mail to the User stating that the User is or will be deprovisioned. (8) Changing: Confirm the User's information system(s) has or will be deprovisioned by comparing the Functional Owner(s) confirmation e-mail(s) with the original DD Form 2875 request on file to Confirm the User's information system(s) has or will be deprovisioned by comparing the Information Owner or office designated by the Information Owner's confirmation e-mail(s) with the original DD Form 2875 request on file.

1. Background. As a result of a Financial Improvement and Audit Readiness (FIAR) Audit in April 2014 on an AFSC managed information system, it was determined that there were ineffective access controls that could result in unauthorized access. The ineffective access controls could potentially exist across all AFSC managed information systems. The attached AFSC Instruction was developed to address the long-term problem by implementing a standard repeatable process to manage/control access to information systems across AFSC.

2. Roles and Responsibilities.

2.1. **User (Information System (IS) Authorized User).** Any individual with the required clearance and a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

2.2. **Supervisor of IS User.** The User's first-level or second-level government Supervisor.

2.3. **Organization Security Manager/Monitor.**

2.3.1. Implements the personnel security program within the organization and provides support to the servicing security activity.

2.3.2. Appointed in writing and oversees security activities for each person assigned to an organization.

2.4. **Organization Information Assurance Officer (IAO) or Appointee.**

2.4.1. Manages the Computer Security (COMPUSEC) Program for the organization.

2.4.2. Requests network access for organization Users.

2.5. **Information Owner.** Manages AFSC Center-level policy, business processes, and functional systems requirements for a specific information system and responsible for approving access to this information system.

2.6. **System Information Assurance Officer (IAO).**

2.6.1. Manages the COMPUSEC Program for a specific IS including monitoring IS activities, and ensuring that the IS is operated, maintained, and disposed of according to security policies and practices.

2.6.2. Ensures compliance with regulatory requirements to include access to the IS.

2.7. **Organization granting system access.** Grants access to specific DoD ISs based on a System IAO or Information Owner request (e.g. DISA).

3. Process for provisioning/deprovisioning of AFSC managed information systems.

3.1. **Provisioning (Access to an Information System)**

3.1.1. **User Will:** Fill out the DD Form 2875 request or system specific form IAW the form's instructions. In the DD Form 2875 request, the user provides justification stating his/her duties as it relates to requesting access to the specific IS (blk #13). Providing a justification such as "access is required to perform my job" is unacceptable and access will be denied. In some cases, the Information Owner provides additional justification on the specific roles for a system (see blk #27 in Attachment 2). Once completed, the User will sign the DD Form 2875 request and forward to the User's Supervisor.

3.1.2. **Supervisor of IS User will:** Review the User's DD Form 2875 request to ensure it is correctly filled out. Specifically, the Supervisor will ensure the DoD Information Assurance CyberAwareness Challenge (blk #10) is current, justification for access is sufficient (blk #13) and the User signed the DD Form 2875 request. Once approved, the Supervisor will sign the DD Form 2875 request (blk #18) and it is then sent to the Organization Security Manager/Monitor. The Supervisor or designated individual will maintain a copy of the DD Form 2875 request to ensure proper deprovisioning of the IS

occurs such as when the User out-processes. Note: If applicable, by placing the DD Form 2875 request in the User's personnel folder it will ensure the list of systems stays with the User if the Supervisor or User leaves or moves offices.

3.1.3. **Organization Security Manager/Monitor will:** Complete the background investigation, date of investigation, and clearance level (blks #28 a,b,c). Once completed, the Organization Security Manager/Monitor will sign the DD Form 2875 request(blk # 31) and send it back to the User.

3.1.4. **User will:** Forward the completed DD Form 2875 request to the System IAO or appointed system access authority. If the System IAO is unknown, the User will contact the system's Information Owner (Note: For some systems, the AF Portal Applications A-Z can be used to find the Information System POC).

3.1.5. **System IAO or Appointed System Access Authority will:** Accept and review the DD Form 2875 request to ensure the User meets the security requirements for the information system. Once approved, sign the DD Form 2875 request (blk #22). The System IAO or appointed system access authority will then send the DD Form 2875 request to the Information Owner.

3.1.6. DELETED

3.1.7. **Information Owner or office designated by the Information Owner will:** Review the DD Form 2875 request for completeness and specifically ensure the User is authorized to have access based on the User's justification stating his/her duties as it relates to requesting access to the information system. Once approved, the Information Owner or office designated by the Information Owner will sign the DD Form 2875 request (blk # 21) and then request system access to the organization granting access (i.e. DISA).

3.1.8. DELETED

3.1.9. **Organization granting system access will:** Grant access and send notification to the User that he/she has system access.

3.1.10. **User will:** Be held responsible for maintaining a list of the approved, accessed systems for deprovisioning purposes (e.g. keep the confirmation emails, maintain copies of DD Form 2875 request, keep a list etc.).

3.2. **Deprovisioning (Removal from an Information System)**

3.2.1. **User will:** Send an e-mail to the Information Owner or office designated by the Information Owner to request deprovisioning from the system.

3.2.2. **Information Owner or office designated by the Information Owner will:** Request to deprovision the User and send a confirmation e-mail to the User stating that the User is or will be deprovisioned.

3.2.3. **User will:** Provide the Supervisor the confirmation e-mail(s). If the User is out-processing, the User will attach the e-mail(s) to the out processing checklist.

3.2.4. **Supervisor will:** Confirm the User's information system(s) has or will be deprovisioned by comparing the Information Owner or office designated by the Information Owner's confirmation e-mail(s) with the original DD Form 2875 request on

file. If the User is out-processing the Supervisor will sign the User's out-processing checklist and attach the confirmation emails.

3.2.5. **User will:** Provide signed out-processing checklist to the Organization IAO showing Supervisor signature. Note: If the User is unable to physically do so (e.g. death, forced removal etc.), the Supervisor will be responsible for deprovisioning the User's IS(s).

3.2.6. **Organization IAO or Appointee will**: Confirm IS deprovisioning has or will be completed in coordination with the User's Supervisor and verifies User account deprovisioning on the out processing checklist.

3.2.7. **Organizations will:** Ensure deprovisioning Users from ISs is included in the unit's out-processing procedures. Below are a few examples of verbiage that may be used on the out processing checklist for the Supervisor and Organization IAO:

3.2.7.1. Supervisor has confirmed the User has been properly deprovisioned from all ISs

3.2.7.2. Organization IAO has verified the User has been properly deprovisioned from all ISs.

3.3. **Sustainment Information System Controls**

3.3.1. Out Processing Checklist

3.3.2. Automated or manual check of the systems' Users every 30 days is required and any inactive users who have not accessed the system during this time frame will be suspended or deprovisioned.

3.3.3. If specified in higher headquarter guidance or the specific information system's security plan, an annual reconciliation is also required.

STEVEN K. ALSUP, SES, AFSC-LG
Director of Logistics, Air Force Sustainment Center

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 33-282, *Computer Security (COMPUSEC)*, 27 March, 2012

MPTO 00-338-5004, *Access Control for Information Systems*, 6 March, 2012

AFMC CII 14-01, *Cybersecurity Access Control*, 1 September 2014

DD Form 2875, *System Authorization Access Request (SAAR)*, August 2009

DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*, 12 March 2014

AFI 33-210, *Air Force Certification and Accreditation (C&A) Program (AFCAP)*, 23 Dec 08

Adopted Forms

DD Form 2875, *System Authorization Access Request (SAAR)*

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AFCAP —Air Force Certification and Accreditation (C&A) Program

AFSC —Air Force Sustainment Center

COMPUSEC —Computer Security

DISA —Defense Information Systems Agency

eMASS —Enterprise Mission Assurance Support Service

ERMS —Electronic Management Record System

IAM —Information Assurance Manager

IAO —Information Assurance Officer

IS —Information System

POC —Point of Contact

PMO —Program Management Office

RMF —Risk Management Framework

SAAR—System Authorization Access Request

Attachment 2

DD FORM 2875 EXAMPLE BLOCK 27

DD Form 2875 Example Block 27

26. NAME *(Last, First, Middle Initial)*

27. OPTIONAL INFORMATION *(Additional information)*

Please mark [X] the appropriate JUSTIFICATION & ACCESS.

User Type	User Group
[ ] A	ALC WRM MONITOR
[ ] D	ALC Inventory Management Division Supervisor
[ ] S	SPD
[ ] I	Inventory Management Specialist
[ ] E	Equipment Specialist
[ ] L	Weapon System Assessor
[ ] M	MAJCOM User
[ ] R	Read-only User

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION		28a. DATE OF INVESTIGATION *(YYYYMMDD)*	
28b. CLEARANCE LEVEL		28c. IT LEVEL DESIGNATION ☐ LEVEL I ☐ LEVEL II ☐ LEVEL III	
29. VERIFIED BY *(Print name)*	30. SECURITY MANAGER TELEPHONE NUMBER	31. SECURITY MANAGER SIGNATURE	32. DATE *(YYYYMMDD)*

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED *(YYYYMMDD)*	PROCESSED BY *(Print name and sign)*	DATE *(YYYYMMDD)*
DATE REVALIDATED *(YYYYMMDD)*	REVALIDATED BY *(Print name and sign)*	DATE *(YYYYMMDD)*

DD FORM 2875 (BACK), AUG 2009 Reset