BY ORDER OF THE COMMANDER
552D AIR CONTROL WING (ACC)

552 AIR CONTROL WING
INSTRUCTION

33-101

21 FEBRUARY 2017

Communications

GROUND SUPPORT SYSTEMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 552 ACNS/SCO

Certified by: 552 ACG/CC
(Colonel Dominic A. Setka)
Pages: 18

This publication implements Air Force Policy Directive 33-1, 9 August 2012, Cyberspace Support. This instruction provides guidance covering basic responsibilities pertaining to AWACS removable media, magnetic media support, chat accounts, and mission data archiving both at home station and at deployed locations under the command of the 552 ACW. Contact supporting records manager as required. This instruction is directive and applies to all units assigned to the 552d Air Control Wing (552 ACW). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication, route AF Form 847s through publications/forms managers. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW AF Manual (AFMAN) 33-363, Management of Records, and disposed of IAW Air Force Records Information System (AFRIMS) Records Disposition Schedule (RDS) or any updated statement provided by the AF Records Management office (SAF/CIO A6P).

1. Iron Key Flash Media Drive (IK)/Removable Media Assembly (RMA)/Onboard-Off board Media (OOM) mission kit (hereinafter referred to as "mission kit") check-out/check-in.

1.1. Tinker AFB.

1.1.1. 552 ACNS/SCOO (hereinafter referred to as "SCOO") responsibilities:

1.1.1.1. Provide the mission crew with a sealed mission kit for acceptance and an "AWACS Mission Recording/IK/RMA/OOM Kit Computerized Transfer Logs" (hereinafter referred to as "Mission Kit Transfer Log") for signature, immediately upon pick up from SCOO. If the kit was not sealed as prescribed in paragraph 1.1.2.1.4, the mission crew must inventory the kit before signing the "Mission Kit Transfer Log." The log can be found on 552 ACNS SharePoint: SCO Operations > Document Management > SCO Historical Documents > SCOO > Admin > Logs > Mission Kit Logs.

1.1.1.2. Check the "Mission Kit Transfer Log" and records any problems encountered.

1.1.1.3. Educate the mission crew or other authorized technician on proper handling procedures for IK/RMA/OOM, which must be handled with extreme care due to fragile parts. Mission kit cases are not considered ruggedized.

1.1.1.4. Review mission kits partition folders, listing all current software and database versions, making sure they are accurate and up-to-date per Software Release Letter provided by 552 ACNS/SCXP. The partition folders will be included in the mission kits.

1.1.1.5. Temporarily secure and store the mission kit until mission crew pick up.

1.1.1.6. The mission crew will conduct an inventory of the mission kit and sign the "Mission Kit Transfer Log" acknowledging transfer of the kit upon pickup.

1.1.1.7. Inventory mission kit and conduct visual check for any damage when returned by crew members. Ensure the mission crew annotates any mission kit problems on the "Mission Kit Transfer Log."

1.1.1.8. Damaged or faulty mission kits that do not pass SCOO internal recovery procedures will be turned in to base supply system using AF Form 2005, Issue/Turn-In Request. New and/or repaired mission kits will be entered into the IK/RMA/OOM electronic database.

1.1.1.9. Track all mission kits by serial number and storage location.

1.1.1.10. Off-load data from the mission kit drives upon return and save the data to the designated network drive. All data will be removed from the drives unless otherwise instructed by the mission crew or authorized technician. Upon turn in, mission crews can request for their kits to be sealed for future use.

1.1.1.11. SCOO will verify, prepare, and certify by initial on the "Mission Kit Transfer Log" that all IK/RMA/OOM placed in the mission kit prior to the inventory by aircrew personnel are operationally ready.

1.1.1.12. Mission Kit Transfer Logs will be maintained for 90 days.

1.1.2. Tinker AFB Mission Crews.

1.1.2.1. The Air Control Network Squadron (ACNS) Operations Officer (Operations Officer refers to any personnel that handle transactions with ACNS/SCOO on behalf of the mission crew, usually the Computer Display Maintenance Technician (CDMT), Communications Technician (CT), or System Technician (ST) (hereinafter referred to as "mission crew") responsibilities.

1.1.2.1.1. Provide SCOO a monthly list of mission crews authorized to pick up mission kits.

1.1.2.1.2. The ACNS Security Managers will verify user clearances and Access Lists.

1.1.2.1.3. Provide mission requirements for mission kit(s) to SCOO no less than 12 hours prior to pick up using the Mission Kit Reservation Checklist. Extenuating circumstances and requests will be handled on a case by case basis.

1.1.2.1.4. The AACS Operations Officer will verify the mission crew is authorized to accept mission kits and that the mission crew reports to SCOO, Network Operations (Building 284, Room 108) to verify that the mission kit contents match the information listed on the "Mission Kit Transfer Log." In addition, the mission crew will check the RMA, OOM, and/or IK for damage. If the kit is being sealed for future use, the mission crew will verify the seal numbers, seal the kit, and sign the "Mission Kit Transfer Log."

1.1.2.1.5. The mission crew must be prepared to pick up and take the mission kit to the aircraft using crew transportation. SCOO will provide over-the-counter Window service only, and will not transport mission kits.

1.1.2.1.6. Return the mission kits at the end of the mission to SCOO. If the mission kits are not checked in within 24 hours of sortie completion, the AACS Operations Officer will be contacted and requested to recover the mission kit.

1.1.3. 552 ACW SIM Maintenance and 552 ACNS/SCT responsibilities:

1.1.3.1. Provide 552 ACNS/SCOO a monthly list of authorized personnel to pick up mission kits.

1.1.3.2. The ACNS Security Managers will verify user clearances and Access Lists.

1.1.3.3. The requesting entity will deliver the mission kit requirements to 552 ACNS/SCOO 12 hours prior to pick up using the "Mission Kit Reservation Checklist." (Attachment 2). Extenuating circumstances and requests will be handled on a case-by-case basis

1.1.3.4. The technician authorized to accept a mission kit will report to SCOO, Building 284, Room 108, to verify that the mission kit contents match the information listed on the "Mission Kit Transfer Log."

1.1.3.5. The authorized technician will check the mission kit for damage. If the kit is being sealed for future use, the technician will verify the seal numbers, seal the kit, and sign the "Mission Kit Transfer Log."

1.1.3.6. The authorized technician will take the mission kit to the required destination using their own modes of travel. SCOO will provide over-the-counter Window service only.

1.1.3.7. The authorized technician will accept the sealed mission kit and sign the "Mission Kit Transfer Log" immediately upon pick up from SCOO. If the mission kit is not sealed as prescribed in paragraph 1.1.2.1.4, the technician must inventory the kit before signing the "Mission Kit Transfer Log."

1.1.3.8. The technician will return the mission kits to SCOO and ensure any problems encountered are annotated on the "Mission Kit Transfer Log."

1.2. Exercises and Deployments.

1.2.1. Exercise and Deployment Media Repository Center (MRC) Responsibilities:

1.2.1.1. Exercise and Deployment locations will maintain/issue media kits from their respective area of operation's MRC. Exercise and deployment locations will implement and maintain programs ensuring access, accountability/inventory, and maintenance for all physical and digital media.

1.2.2. The AACS responsibilities in an exercise or deployed environment:

1.2.2.1. The AACS Operations Officer will provide the deployed unit's senior 552 ACNS liaison officer a list of mission crew members authorized to pick up mission kits.

1.2.2.2. The mission crew will return the mission kits at the end of the mission to the MRC and ensure any problems encountered are annotated on the "Mission Kit Transfer Log."

1.3. Geographically Separated Mission Crews.

1.3.1. Geographically separated mission crews include crews located at the following locations that are supported by the 552ACNS/SCOO:

1.3.1.1. Elmendorf AFB AK

1.3.1.2. Kadena AB Japan

1.3.1.3. AFCENT AOR

1.3.2. Geographically separated locations will maintain/issue media kits from their respective area of operation's MRC. The locations will implement and maintain programs ensuring access, accountability, inventory, and maintenance for all physical and digital media.

1.3.3. The mission crew will return the mission kits at the end of the mission to the tape library and ensure any problems encountered are annotated on the "Mission Kit Transfer Log."

2. Magnetic Media:

2.1. Magnetic Media Control.

2.1.1. Only SCOO personnel will add or remove IK/RMAs/OOMs from magnetic media inventory storage at SCOO.

2.1.2. Mission crews will only use IK/RMAs/OOMs supplied by SCOO. GSU MRCs will verify accountability in local inventory for all IK/RMAs/OOMs received from or shipped to SCOO.

2.1.3. Tinker AFB.

2.1.3.1. 552 ACNS/SCOO Media Operations NCOIC will conduct an annual 100% hands-on inventory of all magnetic media stored at Tinker AFB no later than 15 September of each calendar year.

2.1.3.1.1. The annual inventory will consist of verifying that all magnetic media stored in SCOO are properly accounted for in the IK/RMA/OOM database and that entries in the IK/RMA/OOM database accurately correspond to magnetic media stored in Building 268.

2.1.3.1.2. The annual inventory will consist of verifying 100 % of the IK/RMAs/OOMs that the SCOO is responsible for are accounted for.

2.1.3.1.3. The Media Operations NCOIC will, by Memorandum for Record, inform the 552 ACNS/SCO Flight Commander and 552 ACNS Commander of completion and results of annual inventory.

2.1.4. All other locations.

2.1.4.1. MRC locations geographically separated from Tinker AFB must keep an electronic inventory/archive log.

2.1.4.2. Media Librarians will accomplish magnetic media inventories using the IK/RMA/OOM electronic database inventory at all sites during personnel rotations.

2.1.4.2.1. The MRCs will provide SCOO with an electronic or faxed copy of the final inventory (signed by both incoming and outgoing personnel) prior to departing the deployed location.

2.1.4.2.2. The returning technician will note discrepancies and return the listing to 552 ACNS/SCOO within 12 hours of arriving at Tinker AFB.

2.2. Mission Archiving Responsibilities.

2.2.1. 552 ACNS/SCO Flight Commander, deployed commanders, and detachment commanders in deployed locations are responsible for ensuring personnel adhere to established labeling and archiving procedures as directed by the 552 ACW Commander. The following naming convention will be used at all locations: ‘missionnumber_tailnumber’ (ex: k3c312_0008)

2.2.2. Once mission kits are returned to SCOO, the recorded data contained on those mission kits will be copied to local network storage.

2.2.2.1. As network storage space requirements mandate, mission recordings will be archived to magnetic media for long-term storage. This data will then be removed from local network storage.

2.2.2.2. Mission data stored in this manner will be retained for ten (10) years unless otherwise directed by 552 ACW/CC, 552 ACW/CV, or HQ ACC.

2.2.3. Mission archives from forward deployed that are over 90 days old will be delivered via tail swap or couriered to 552 ACNS/SCOO.

2.2.3.1. The MRC will provide 552 ACNS/SCOO with a complete inventory of all items sent. Additionally, the MRC must provide SCOO the courier information (Name, Rank, estimated arrival date and contact info) before the courier departs with media.

2.2.3.2. Upon delivery to 552 ACNS/SCOO, the mission archives will be verified against the inventory, logged, labeled with the respective operation and stored as stated in para 2.2.2.2.

2.2.4. Accessing Mission Archives.

2.2.4.1. All mission archives are classified SECRET.

2.2.4.2. Only 552 ACNS/SCOO personnel will have access to archive storage area.

2.2.4.3. Individuals assigned to the 552 ACW are authorized to request copies of missions only after their access has been validated by the 552 ACNS Security Manager.

2.2.4.4. All mission media or archives leaving SCOO control must be requested through SCOO, signed out using AF Form 310, and tracked until returned to SCOO control.

2.2.4.4.1. Any mission medium or archive authorized to be sent outside of Tinker AFB will be signed out on AF Form 310 and tracked until verification is sent confirming delivery. All mission media or archives leaving the possession of 552 ACNS/SCOO will be copies of the original; the originals will remain in 552 ACNS/SCOO control at all times.

2.2.4.4.2. Mission archives located in deployed locations will be controlled by the deployed MRC at all times. Deployed MRC are authorized to release copies of mission archives only to approved personnel, couriers, or mission crews on the list maintained by the Communications OIC. Original archive media will not be released but will remain under the control of the deployed MRC at all times.

2.2.4.5. Under no circumstances will mission media be released to unauthorized individuals.

3. Account Processes.

3.1. Information within the organization is potentially vulnerable to access and exploitation by individuals using active accounts that should have been deactivated. This includes individuals who have transferred from the organization, had their employment terminated, lost appropriate security clearance/need-to-know, or who otherwise are no longer authorized access to the system or its information resources. In order to prevent unauthorized access and potential loss/compromise/destruction of information, it is essential that accounts be properly controlled and restricted only to authorized users.

3.2. Privileged and non-privileged account holders play a critical role in ensuring the security integrity of systems maintained by 552 ACNS personnel. The following procedures are accomplished to maintain a secure posture.

3.3. Unit Commanders will:

3.3.1. Require users that need an account on one or more systems administered within 552 ACNS/SCOO to request access from the servicing administration team in building 284, where they will receive full documentation and guidance on completion.

3.3.2. Require an entry on the unit's out processing sheet for users PCS'ing, PCA'ing, retiring, separating, etc., to out-process with 552 ACNS/SCOO to delete their account(s).

3.3.3. Require that personnel who have security clearances revoked or suspended are immediately identified for account suspension/deletion.

3.4. 552 ACNS/SCOO System Administrator responsibilities:

3.4.1. Configure all systems in accordance with applicable Defense Information Systems Agency Security Technical Implementation Guides, the 552 ACNS Information Assurance Plan, vendor provided installation and configuration guides, and any other applicable security instructions as deemed appropriate by the 552 ACW Information Assurance Office.

3.4.2. Create user accounts; the user sets password if available at that time, otherwise the user will coordinate with the 552 ACNS/SCOO to reset the password.

3.4.3. If a user forgets his/her password, System Administrators will work with the user in person to reset the password. System administrators will positively verify the account holder's identity prior to resetting the password.

3.4.4. Monitor systems for account inactivity. Suspend inactive accounts after 90 days of inactivity. Delete accounts after 1 year of inactivity.

3.4.5. 552 ACNS/SCO system administrators will disable user IDs and passwords within 90 days of notification that a user no longer requires or is authorized system access, accounts will be deleted at 180 days.

3.4.5.1. 552 ACNS/SCO system administrators will disable any user accounts that have been inactive for 90 days or more, accounts will be deleted at 180 days.

3.4.5.2. 552 ACNS/SCO system administrators will immediately disable any account through which unauthorized user activity has been detected.

3.5. Account holders will:

3.5.1. Protect their user credentials, e.g., not share account passwords with anyone, to include system administrators.

3.5.2. Use appropriate strength passwords in accordance with the system's ability and requirements. For most systems, this requirement is a 14-character minimum length and two each of uppercase letters, lowercase letters, numbers, and special characters.

3.5.3. Out-process (PCS/PCA/TDY/Deployments etc.) through 552 ACNS/SCOO to delete/suspend the user account.

3.5.4. Notify System Administrators and IAMs/IAOs immediately when system access is no longer required or are authorized system access has been revoked.

3.6. 30/35 Networks ("Mainframe", "ClassLAN")

3.6.1. All accounts on the Mainframe and ClassLAN will be individual accounts. There will be no "group" accounts designed for multiple personnel to log on the system.

3.6.2. Personnel requiring an account must complete a DD Form 2875, System Authorization Access Request, obtain appropriate signatures, and bring to 552 ACNS/SCOO for account creation. The latest version of the form is available from the following DoD site: **http://www.dtic.mil/whs/directives/forms/eforms/dd2875.pdf**

3.6.3. To facilitate automation on the mainframe, account names use a two-letter and two-digit format. The same account name is used for both systems: mainframe and ClassLAN, however, different passwords will be used for the two systems. The account holder's additional information (name, rank, office symbol) are included in account properties areas.

3.7. 40/45 Ground Support System /Deployable Ground System (GSS/DGS)

3.7.1. The AWACS 40/45 GSS/DGS information system access is gained through the presentation of an individual identifier (e.g., a unique token or user logon ID) and password.

3.7.2. Personnel requiring an account must complete a DD Form 2875, System Authorization Access Request (Figure 1), obtain appropriate signatures, and bring to 552 ACNS/SCOO for account creation.

3.7.3. Account names use a <firstname.lastname> format. Account passwords must meet the following minimum standards: a case sensitive, 14-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each. At least four characters must be changed when a new password is created.

3.7.4. Group Identification and Authentication is not authorized. Any deviations from this policy must be completed in accordance with the 552 ACW Information Assurance Plan and will be evaluated on a case-by-case basis.

3.8. Tinker Network Entry Point (TNEP)/Transitional Network Capability (TNC)

3.8.1. The TNEP uses two types of accounts, individual identifying accounts and group accounts. Personnel with privileged accounts, e.g., system administrators, security administrators, etc., will only use an individually identifying account (example: john.doe). Group accounts are intended for mission use only.

3.8.2. Group Accounts

3.8.2.1. Group account names are defined by the 552 OSS/OSK. Group account passwords are managed by 552 ACNS/SCOO under guidelines presented by the Approval to Operate (ATO).

3.8.2.2. Validation of Security Clearance:

3.8.2.2.1. The 552 Operations Group (OG) and 552 Maintenance Group (MXG) will provide 552 ACNS with a Pickup Authorization Letter IAW 552 ACNS/SCOO RMA OPERATING INSTRUCTION, 3 MARCH 2010. The Pickup Authorization Letter lists those individuals whose Security Clearance has been verified and is authorized to pick up classified materials from 552 ACNS. The letter is updated whenever a crewmember or maintenance personnel change occurs. All personnel on the list will be vetted by the ACNS Security Managers will verify user clearances and Access List using Joint Personnel Adjudication System (JPAS) before user is granted access to a TNEP account.

3.8.2.2.2. Group account authorization: Due to the unique operational requirements associated with TNC and TNEP, group accounts are authorized for use. There are three types of group accounts that 552 ACNS will manage: TNC Max-Pac local login, TNEP Remote Access Server (RAS) login, and TNEP Chat Server login. These are all at the Classified SECRET level and must be treated accordingly.

3.8.2.3. Group accounts and passwords are issued by 552 ACNS/SCOO when the aircrew or maintenance person picks up the "kits" for the mission or maintenance.

3.8.3. Account Management: 552 ACNS system administrators will create group accounts IAW 552 ACNS Mission Kit Reservation Checklist. Passwords for the TNEP RAS authentication will meet all the requirements for SIPRNet passwords; e.g., at time of this instructions publication: 14 characters, two each of uppercase, lowercase, number, and special character. The TNEP server enforces password complexity, immediate reuse, and requirement to change passwords at least every 60 days.

3.8.4. TNC Max-Pac accounts are associated with the seat position on the aircraft where the TNC is located for the username (e.g. seat1, seat2). All TNC Max-Pac will have the same image and therefore will not have unique usernames and passwords for each aircraft.

3.8.5. TNEP RAS user accounts are associated with the associated host base, kit number, and front or back seat/row. There are two Iridium data links per aircraft. Therefore, there will be two unique accounts created per aircraft and will have passwords created IAW para 4.7.3, meeting SIPRNet password standards.

3.8.6. Chat server user accounts will be determined by the 552 OG to meet mission requirements. After authenticating through the TNEP RAS, users will proceed to log into the Chat server. 552 OSS/OSK, via 552 OSS/OSR, will provide usernames IAW tactical chat information transfer protocol that are managed as part of the configuration control board. The operator logs in with the appropriate username (e.g. "call-sign") for the mission. Passwords for all chat server accounts will be created IAW para 4.7.3.

3.8.7. 552 ACNS system administrators will maintain a current list of all accounts and passwords and will mark document as SECRET. The account list document is issued per para 3.2.1 of this instruction as part of the TNC drive kit.

3.8.7.1. The expiration date of accounts/passwords will be documented on the account and password document when issued to the end user. This ensures situational awareness for 552 ACNS, 552 OG and 552 MXG personnel who issue and utilize the accounts. Future passwords can be provided to aircrew on request as necessary to support deployed situations.

3.8.7.2. 552 ACNS system administrators will change expiring passwords and publish a new account and password list on a monthly basis. Old account lists, passwords, and copies must be destroyed IAW established policies. If accounts are no longer required, they must be removed from the system within 48 hours of notification.

3.8.7.3. 552 ACNS system administrators will conduct password resets monthly and on an as-needed basis.

3.8.7.4. 552 ACNS system administrators will audit for inactive accounts. Accounts are considered inactive if not used for 90 days and will be suspended. Systems administrators will maintain situational awareness of deployed, TDY, depot phase, etc. aircraft and suspend those accounts accordingly.

3.8.8. Individual Identifying Accounts.

3.8.8.1. All privileged accounts will use an individual identifying account name, e.g., john.doe.

3.8.8.2. Personnel possessing an individual account will not share account password with other personnel.

3.8.8.3. Privileged accounts will not be configured for dial-in capabilities. Individuals with privileged accounts who also require dial-in capability will be provided a separate non-privileged account with dial-in rights.

3.8.8.4. Personnel requiring an individual account will complete a DD Form 2875, System Authorization and Access Request. Completed forms will be delivered to 552 ACNS/SCOO for account creation.

3.8.8.5. Disable and remove user IDs and passwords within 72 hours of notification that a user no longer requires or is authorized system access.

3.8.8.6. SCOO System Administrators shall suspend user accounts that have been inactive for 30 days or more.

3.8.8.7. SCOO System Administrators shall immediately disable any account through which unauthorized user activity has been detected.

4. Mission Planning Cell (MPC)/Post Mission Processing Cell (PMPC).

4.1. Tinker AFB Building 284.

4.1.1. The 552 ACNS/SCOO will be responsible for maintenance & security of the 40/45 MPC/PMPC located in Building 284.

4.1.2. Authorized personnel using the MPC will be responsible for security while in the room and will coordinate with the 552 ACNS/SCOO at 734-3195. One individual will maintain security until the 552 ACNS/SCOO personnel has assumed responsibility of the room for shut down operations.

4.1.3. Room scheduling will be accomplished by contacting 552 ACNS/SCOO at (405) 734-3195 or (405) 734-3071 to determine room availability and hours of operation. Users will request the number of workstations required due to the initial availability and multiple requests for the MPC.

4.1.4. Work station priority will be in the following order:

4.1.4.1. Mission planning

4.1.4.2. 552 ACNS use

4.1.4.3. Aircrew debriefing

4.1.4.4. A minimum of one workstation will be reserved for 552 ACNS use for initial configuration management.

4.2. GSS Remote Terminals.

4.2.1. The 552 ACNS/SCOO will be responsible for maintenance of the 40/45 MPC/PMPC located across the 552 ACW campus on Tinker AFB.

4.2.1.1. EGS will consist of the following 552 ACNS/SCOO maintained equipment:

4.2.1.1.1. Network Switch

4.2.1.1.2. TACLANE Encryption Device and associated User Crypto Ignition Key (CIK)

4.2.1.1.2.1. 552 ACNS personnel will provide annual re-key of all TACLANE Encryption Devices.

4.2.1.1.3. Thin Client User Terminals

4.2.2. The owning unit must establish policy to ensure the security of terminals located within their facilities.

4.2.2.1. The TACLANE User CIK must be secured in a GSA approved Class 6 Security Container when not in active use. Alternately, the CIK may be stored in any area cleared for open storage of Secret data.

4.2.2.2. The Thin Client User Terminals do not store classified data and are not required to be secure during non-duty hours. Once setup, these devices may be left in place.

4.2.3. Accounts are established in accordance with the procedures outlined in paragraph 3.7.

4.2.4. Users should contact the 552 ACNS/SCOO 40/45 Team with any questions or concerns during duty hours. After duty hours, users can contact the 552 ACNS Communications Focal Point on-call phone at (commercial) (405) 210-8428.

DAVID M. GAEDECKE, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFMAN 33-363, *Management of Records,* 1 March 2008

Adopted Forms

AF Form 310, *Document Receipt and Destruction Certificate*

AF Form 847, *Recommendation for Change of Publication*

AF Form 2005, *Issue/Turn-in Request*

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

Prescribed Forms

Abbreviations and Acronyms

AACS—Airborne Air Control Squadron

ACC—Air Combat Command

ACNS—Air Control Network Squadron

ACW—Air Control Wing

AFCENT—Air Forces Central

AOR—Area of Responsibility

ATO—Approval to Operate

AWACS—Airborne Warning and Control System

CDMT—Computer Display Maintenance Technician

CIK—Crypto Ignition Key

CIO—Chief Information Officer

ClassLAN—Classified Local Area Network

CT—Communications Technician

DGS—Deployable Ground System

EGS—Extended Ground System

GSA—General Service Administration

GSS—Ground Support System

GSU—Geographically Separated Unit

HQ—Headquarters

IAM—Information Assurance Manager

IAO—Information Assurance Officer

IAW—In Accordance With

ID—Identification

IK—Iron Key

JPAS—Joint Personnel Adjudication System

MPC—Mission Planning Cell

MCR—Media Repository Center

MXG—Maintenance Group

NCOIC—Non—Commissioned Officer in Charge

OG—Operations Group

OIC—Officer in Charge

OOM—Onboard-Offboard Media

PCA—Permanent Change of Assignment

PCS—Permanent Change of Station

PMPC—Post Mission Processing Cell

RAS—Remote Access Server

RMA—Removable Media Assembly

SIM—Simulator

ST—System Technician

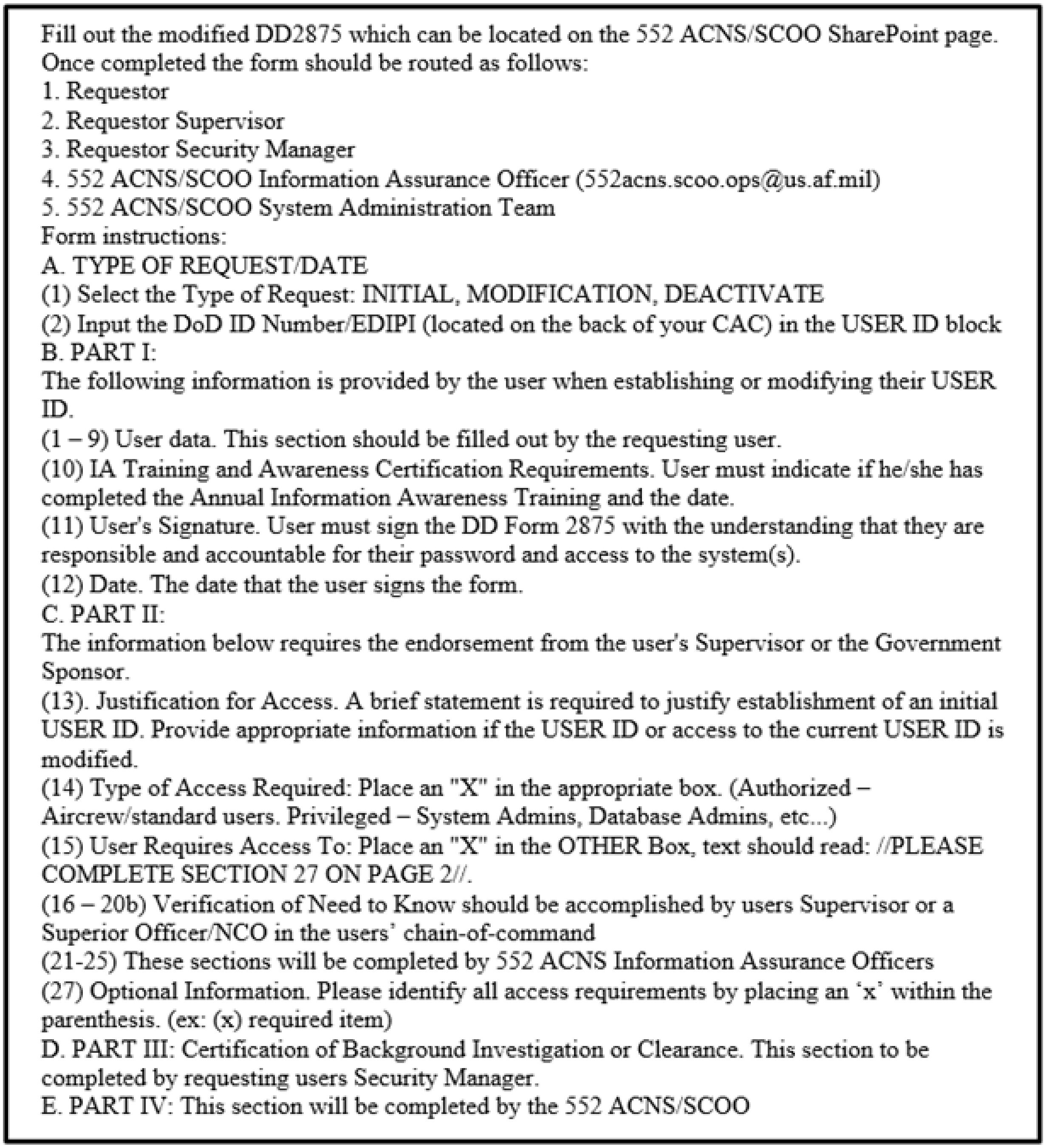
TDY—Temporary Duty

TNC—Transition Network Capability

TNEP—Tinker Network Entry Point

Attachment 2

FIGURE A2.1 INSTRUCTIONS FOR FILLING OUT SAAR



Fill out the modified DD2875 which can be located on the 552 ACNS/SCOO SharePoint page.
Once completed the form should be routed as follows:

1. Requestor
2. Requestor Supervisor
3. Requestor Security Manager
4. 552 ACNS/SCOO Information Assurance Officer (552acns.scoo.ops@us.af.mil)
5. 552 ACNS/SCOO System Administration Team

Form instructions:

A. TYPE OF REQUEST/DATE

(1) Select the Type of Request: INITIAL, MODIFICATION, DEACTIVATE

(2) Input the DoD ID Number/EDIPI (located on the back of your CAC) in the USER ID block

B. PART I:

The following information is provided by the user when establishing or modifying their USER ID.

(1 – 9) User data. This section should be filled out by the requesting user.

(10) IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form 2875 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

C. PART II:

The information below requires the endorsement from the user's Supervisor or the Government Sponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized – Aircrew/standard users. Privileged – System Admins, Database Admins, etc...)

(15) User Requires Access To: Place an "X" in the OTHER Box, text should read: //PLEASE COMPLETE SECTION 27 ON PAGE 2//.

(16 – 20b) Verification of Need to Know should be accomplished by users Supervisor or a Superior Officer/NCO in the users' chain-of-command

(21-25) These sections will be completed by 552 ACNS Information Assurance Officers

(27) Optional Information. Please identify all access requirements by placing an 'x' within the parenthesis. (ex: (x) required item)

D. PART III: Certification of Background Investigation or Clearance. This section to be completed by requesting users Security Manager.

E. PART IV: This section will be completed by the 552 ACNS/SCOO

Attachment 3

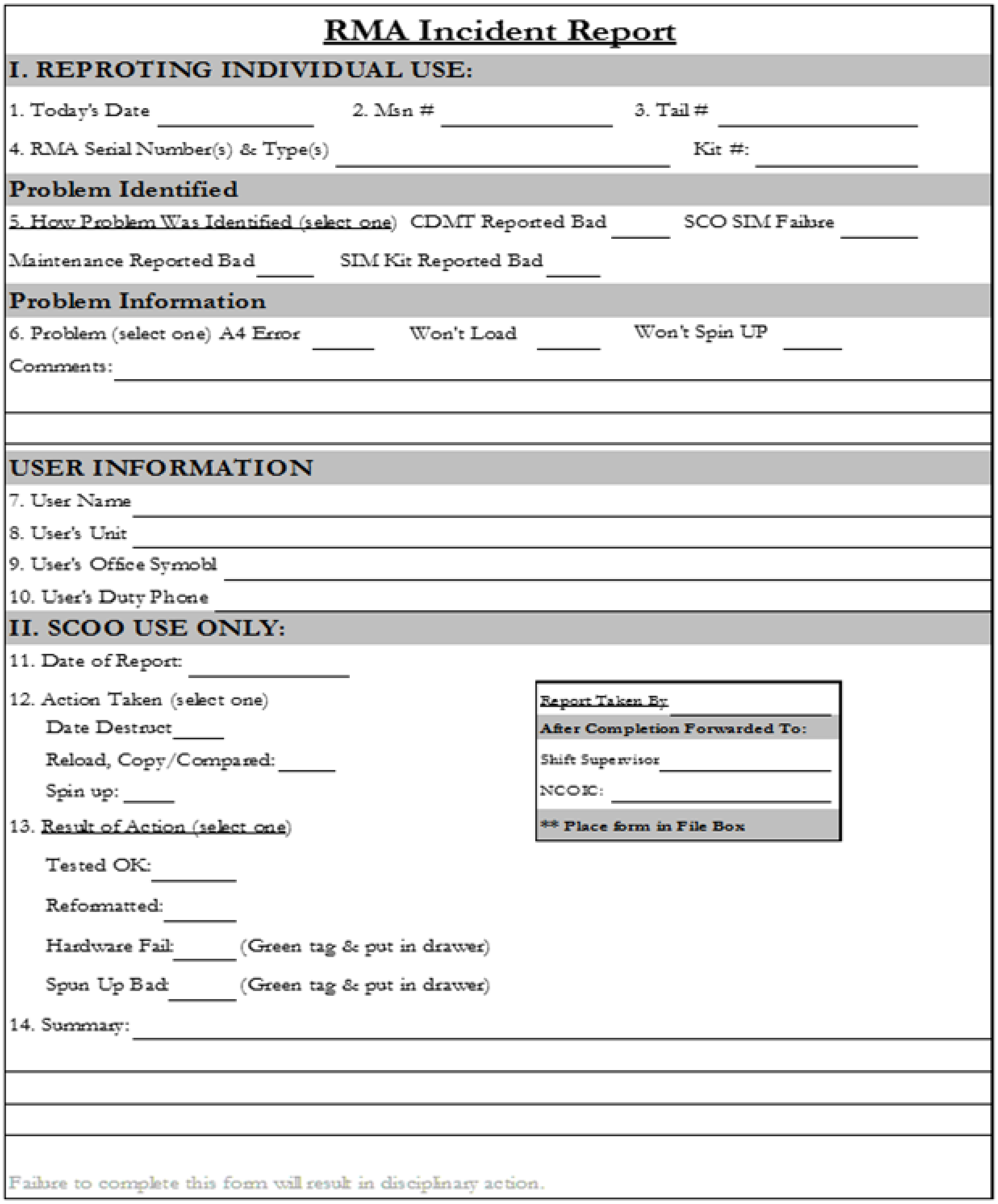
TABLE A3.1 552 ACNS MISSION KIT RESERVATION CHECKLIST.

Today’s Date	
Time	
Requestor	
Unit	
Work #	
Cell #	
Notified by:	
Mission #	
Tail #	
Pickup Date	
Pickup Time	
Return Date	
Return Time	
30/35	
TNC KIT #	
MSN KIT #	
40/45	
OOM Type	( ) DMS 1.5 ( ) DMS 2.0 ( ) DMS 3.0 ( ) BOTH
IRON KEY Drive	( ) YES ( ) NO
RSIP TYPE	( ) USAF 05 ( ) USAF 06 ( ) BOTH
40/45 Media Manager, Kit Status Verification	

REMARKS

Attachment 4

FIGURE A4.1 RMA INCIDENT REPORT.



RMA Incident Report

I. REPROTING INDIVIDUAL USE:

1. Today's Date ________ 2. Msn # ________ 3. Tail # ________

4. RMA Serial Number(s) & Type(s) ________ Kit #: ________

Problem Identified

5. How Problem Was Identified (select one) CDMT Reported Bad ____ SCO SIM Failure ____

Maintenance Reported Bad ____ SIM Kit Reported Bad ____

Problem Information

6. Problem (select one) A4 Error ____ Won't Load ____ Won't Spin UP ____

Comments: ________

USER INFORMATION

7. User Name ________

8. User's Unit ________

9. User's Office Symobl ________

10. User's Duty Phone ________

II. SCOO USE ONLY:

11. Date of Report: ________

12. Action Taken (select one)

Date Destruct ____

Reload, Copy/Compared: ____

Spin up: ____

13. Result of Action (select one)

Tested OK: ____

Refomatted: ____

Hardware Fail: ____ (Green tag & put in drawer)

Spun Up Bad: ____ (Green tag & put in drawer)

14. Summary: ________

Report Taken By ________

After Completion Forwarded To:

Shift Supervisor ________

NCOIC: ________

**** Place form in File Box**

Failure to complete this form will result in disciplinary action.