BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE MANUAL 16-602

18 DECEMBER 2000

Operations Support

THE STRATEGIC ARMS REDUCTION TREATY (START) TRACKING AND REPORTING SYSTEM (STARS) USER MANUAL

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: ACC AOS/AOCF
(TSgt Eric W. Sanborn)
Supersedes AFMAN 16-602, 1 February 1996.

Certified by: HQ USAF/XON
(Maj Gen Franklin J. Blaisdell)
Pages: 23
Distribution: F

This publication outlines responsibilities and procedures for complying with Air Force START notification requirements. It describes how to recognize a reportable event, select, complete and submit the proper notification format using STARS. To ensure a full understanding of START notification reporting requirements, refer to the treaty text. This manual implements DoDD 2060.1, *Implementation of, and Compliance With, Arms Control Agreements,* AFPD 16–6, *Arms Control Agreements* and AFI 16-601, *Implementation of, and Compliance with, Arms Control Agreements.* Supplement this manual at any organizational level. Direct questions or comments on this manual through appropriate MAJCOM channels. MAJCOMs must forward a copy of all supplements to the USAF STARS Central Node, Air Combat Command AOS/AOCF, 205 Dodd Blvd, STE 101, Langley AFB VA 23665-2789.

Failure to observe the provisions of this manual may result in administrative or judicial sanctions including punishment under the Uniform Code of Military Justice.

SUMMARY OF REVISIONS

This manual reflects changes too numerous and extensive to individually list. It is, for all intents and purposes, a new manual. Personnel are urged to carefully review the entire document to familiarize themselves with new and updated information.

Chapter 1

INTRODUCTION

1.1. Read Me First. Read this chapter for general instructions before preparing or interpreting:

1.1.1. STARS responsibilities, training requirements and administrative requirements,

1.1.2. STARS security policy,

1.1.3. Administrative tools, and

1.1.4. START.

1.2. Concept of Operations. AF Strategic Arms Reduction Treaty (START) reporting responsibilities require timely, accurate, and controlled reporting of treaty activities. The START Tracking and Reporting System (STARS) is the system designed to ensure these events are reported to the US Department of State Nuclear Risk Reduction Center (NRRC). This manual provides instructions for complying with START notification requirements.

1.3. Releasability. Releasability of START Treaty information is governed by Joint Compliance and Inspection Commission Agreement Number 17**.** START notifications may only be released to AF agencies with a valid need-to-know and appropriate security clearance. Coordinate all other requests for release through your MAJCOM Treaty Compliance Office and HQ USAF/XONP. (See AFI 31-401, *Managing the Information Security Program*, and AFI 31-501, *Personnel Security Program Management*.)

1.4. Timeliness of Notification. Rapid and accurate submission of required notifications is necessary for the US government to comply with START. The Treaty carries with it the full weight of international law. Submit every STARS notification to meet the unit suspense listed in the format directions. This time is based on a trigger event (e.g., the movement of a heavy bomber or an ICBM). The US Government must transmit the notification to the Other Parties by the time listed under "NRRC suspense."

1.5. Linked Notifications. Some notifications are reported in sequence with prior or follow-on notifications. Use the STARS Workbook Quick Reference Charts, notification directions and the notification sequence charts to submit all required notifications. For assistance, call your unit or MAJCOM Treaty Compliance Office, or the USAF STARS Central Node.

1.6. Supplemental Material. Some notifications require photographs, site diagrams or other supplemental material be provided to the Other Parties through diplomatic channels. Forward supplemental material through appropriate channels within Treaty timelines. All supplemental materials should be processed through Treaty Compliance Offices and HQ USAF/XONP.

1.7. STARS Computer User Manual. The STARS Computer User Manual (SCUM) provides detailed operating instructions for the STARS Personal Computer (PC) and Secure Data Device (SDD). The SCUM guides users through notification processes with tutorials, examples, and computer screen displays.

1.8. STARS WORKBOOK. The STARS Workbook provides detailed instructions for Treaty required notifications and administrative documentation. The workbook will assist users in the completion of required paperwork using examples, sequence charts, and checklists.

1.9. Four Step Reporting. Accomplish STARS reporting using these four steps:

1.9.1. Step 1. Recognize the Treaty reportable event. Use the STARS Notification Sequence Charts located in your STARS workbook to help you recognize and confirm an event is treaty reportable. Call your local Treaty Compliance Office for assistance.

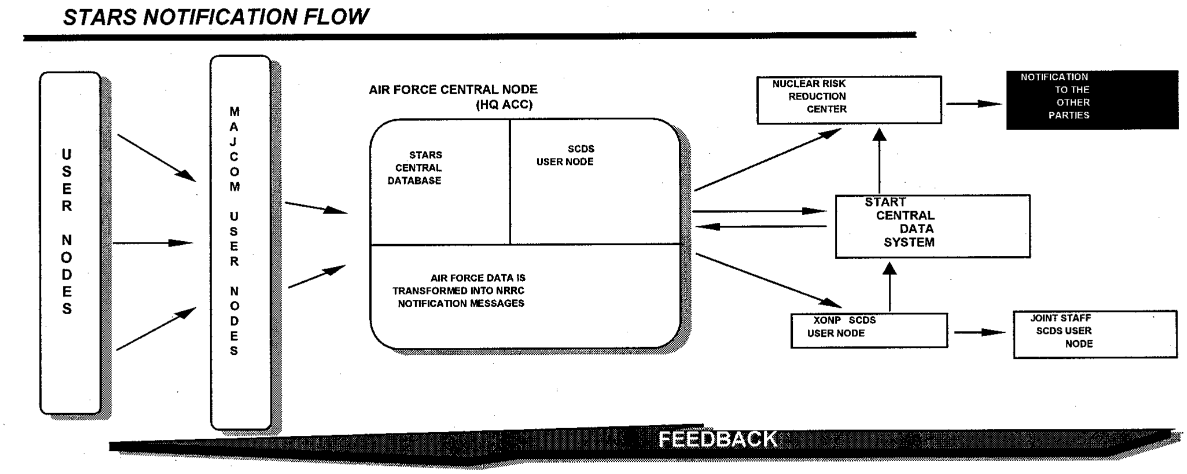
1.9.2. Step 2. Select the correct format(s). Refer to the Table of USAF STARS Notifications in the STARS Workbook.

1.9.3. Step 3. Complete the format(s). Collect the required information and complete the notification. Use Zulu time when submitting a notification and place all remarks on the transmittal letter.

1.9.4. Step 4. Submit the format(s). Use local procedures outlined in your base START Compliance Plan. Forward or transmit the notification to the next level by the unit suspense specified in the format instructions. Should you detect an error in a notification after transmission, contact your MAJCOM or the STARS Central Node immediately for assistance.

1.10. Feedback. After transmission of the notification is complete, the originating unit will receive a copy of the report as submitted from USAF Central Node to the NRRC. You should use this information to verify that the information you transmitted was in fact the information transmitted to the Other Parties. Figure 1.1 shows the notification flow for STARS notifications.

Figure 1.1. STARS Notification Flow.


STARS NOTIFICATION FLOW
USER NODES
MAJCOM USER NODES
AIR FORCE CENTRAL NODE (HQ ACC)
STARS CENTRAL DATABASE
SCDS USER NODE
AIR FORCE DATA IS TRANSFORMED INTO NRRC NOTIFICATION MESSAGES
NUCLEAR RISK REDUCTION CENTER
NOTIFICATION TO THE OTHER PARTIES
START CENTRAL DATA SYSTEM
XONP SCDS USER NODE
JOINT STAFF SCDS USER NODE
FEEDBACK

1.11. Notification Correction. In the event the Central Node receives an incomplete notification or a notification is found to be in error, the Central Node controller will do the following:

1.11.1. Contact the originator and explain the error/omission.

1.11.2. Inform the originator that the notification will be denied and that the originator is responsible for generating a corrected notification.

1.11.3. Deny the original notification.

1.11.4. Ensure a specific reason(s) for denial is stated in the message.

1.11.5. Monitor for and transmit the corrected copy.

1.11.6. The only exception to this notification correction procedure would be if the NRRC suspense time were in jeopardy of being exceeded.

1.11.6.1. If this situation occurs the Central Node controller will do the following:

1.11.6.2. Contact the originator and explain the error/omission.

1.11.6.3. Inform the originator that the Central Node will correct the discrepancy to prevent a Treaty violation.

1.11.6.4. Correct the notification. Ensure the specific error is identified in the “Comments for Originator” window.

1.11.6.5. Transmit the notification to the NRRC.

Chapter 2

RESPONSIBILITIES

2.1. Responsibilities. This manual establishes the following responsibilities and authorities for all users of the STARS.

2.2. HQ USAF/XONP is the OPR for STARS policy and must:

2.2.1. Review, approve and forward applicable notifications and reports received from the Central Node.

2.2.2. Review NRRC-processed reports and manage resolution issues.

2.2.2.1. Provide the USAF Central Node a record copy of additions to the STARS database prior to the requirement to report any new facility or Treaty Accountable Item (TAI).

2.2.2.2. Fund STARS development, deployment, operations and maintenance.

2.2.2.3. Designate, in writing, a System Administrator/Information System Security Manager (SA/CSSO) and one alternate.

2.3. USAF Central Node for STARS (AFCN) is the OPR for STARS operations and must:

2.3.1. Operate STARS on a continuous 24-hour basis.

2.3.2. Designate, in writing, a System Administrator and one alternate. These individuals must attend the USAF STARS Operators Course.

2.3.3. Review, approve and forward notifications to HQ USAF/XONP if the suspense is greater than 48 hours or directly to the NRRC if the suspense is less than 48 hours.

2.3.4. Provide system report information and instructions to STARS user nodes including: policies, procedures, reporting changes, updates and workbook instructions.

2.3.5. Provide feedback from the NRRC and HQ USAF/XONP to STARS user nodes.

2.3.6. Secure accreditation for STARS operations from the Designated Approval Authority (DAA).

2.3.7. Maintain historical records including: audit logs, notifications, problem reports, change requests, mail messages, software release information, and Working Group meeting minutes.

2.3.8. Publish and maintain this manual.

2.3.9. Serve as STARS Subject Matter Expert.

2.3.10. Identify STARS funding requirements to HQ USAF/XONP.

2.3.11. Identify STARS Central Node funding requirements to the host MAJCOM.

2.3.12. Create and maintain the STARS Workbooks and associated reporting aids.

2.3.13. Provide feedback concerning STARS problem reports and change requests.

2.3.14. Test all software releases prior to deployment. This includes development and administration of Air Force specific testing, if applicable.

2.3.15. Ensure all Central Node personnel are fully trained. Training will include the USAF STARS Operators Course and Central Node Master Lesson Guide.

2.3.16. Develop and maintain the Unit Assistance and Training Visit (UA+TV) Plan and procedures. Conduct UA+TV at each STARS node at a minimum of once every 24 months.

2.4. ACC is designated the AFCN host MAJCOM and must:

2.4.1. Provide appropriate manpower positions to operate STARS on a continuous 24-hour per day basis. HQ USAF/XO will fund manpower positions.

2.4.2. Plan, program, and budget AFCN operational funding requirements.

2.5. MAJCOMs must:

2.5.1. Monitor START-related activity and ensure submission of required notifications. Notification procedures will be in accordance with the START Treaty, AFMAN 16-602. STARS workbook(s), and manual reporting procedures.

2.5.2. Designate a System Administrator and one alternate. The SA and ASA are required to attend the STARS Operations Course.

2.5.3. Operate automated and/or manual STARS.

2.5.4. Conduct STARS training using the STARS Master Lesson Plan.

2.5.5. Train all MAJCOM STARS personnel in all applicable areas of responsibilities including: transmission, MAJCOM and node guidance and standby procedures. Determine level of training required for their sub-ordinate units and implement training as necessary. Training should include all unit level processes including: generation, review, database verification, message catalog checks and security procedures.

2.5.6. Review applicable portion of the STARS data-base and correct as necessary.

2.5.7. Plan, program, and budget for STARS operations and training.

2.5.8. Provide the AFCN a report of STARS-related Treaty violations, occurring within their MAJCOM, NLT 5 duty days after the violation. The report must include the unit, TAI/TLI involved, factors leading up to the violation, and corrective action.

2.5.9. Designate an automated STARS node within their MAJCOM to input report data for manual reporting nodes.

2.5.10. Establish procedures for manual reporting nodes. These procedures must ensure notification data is provided to the designated automated STARS node to facilitate submission prior to the unit's suspense.

2.6. Units must:

2.6.1. Monitor START-related activity and submit notifications through their MAJCOM. Notification procedures will be in accordance with START, this manual, the STARS Workbook, MAJCOM Guidance and local procedures provided by the host Treaty Compliance Office.

2.6.2. Designate a System Administrator and one alternate. The SA and ASA are required to attend the STARS Operators Course. More than one ASA can be trained, however, only the SA and primary ASA can have SA level access in STARS.

2.6.3. Track assigned TAI regardless of location. A computer-generated product may be used for this purpose. (See STARS Workbook)

2.6.4. Coordinate changes in TAI assignment prior to the change. Coordination should include affected MAJCOM(s) and all other applicable units.

2.6.5. Review the applicable portion of the STARS central database for accuracy and correct as necessary.

2.6.6. Operate automated and/or manual STARS.

2.6.7. Maintain incoming and outgoing notification logs. A computer-generated product may be used. (See STARS Workbook)

2.6.7.1. As a minimum, log entries should include the format number, date and time in zulu, controllers name, and unit. The results of both the format and compliance check are encouraged, but not mandatory.

2.6.8. Conduct STARS initial and recurring training using the STARS Master Lesson Plan.

2.6.9. Verify generation and submission of Automatically Generated Notifications resulting from the movement or destruction of assigned TAI.

2.6.10. Add STARS hardware and software to the unit Emergency Removal of Classified Plan.

2.6.11. Develop contingency reporting procedures in the event of emergency relocation.

2.6.12. Identify STARS funding requirements to MAJCOM through the Treaty Compliance Office.

Chapter 3

STARS SECURITY

3.1. User Node Security Policy and Procedures—General. The Central Node serves as the STARS manager for security, system administration and configuration management. The Central Node, in support of START, manages user node and MAJCOM notifications for delivery to HQ USAF/XONP and the NRRC. The entire USAF reporting structure and its procedures are encompassed in STARS. This section establishes STARS security policy and procedures. It identifies STARS user node equipment, software, user node System Administrator and Computer System Security Officer (SA/CSSO) Standard Operating Procedures (SOPs), and user SOPs.

3.2. Classification Authority . STARS has an overall classification of SECRET. The classification authority is:

CLASSIFIED BY: OUSD (A&T)/ACI&C, 12 Dec 97 DECLASSIFY ON: DD MMM YY (10 years from date**)**

3.3. Classification. STARS notification formats containing geographic coordinates are Confidential by agreement between the Other Parties and the United States. The SECRET classification applies to the STARS terminal, Secure Data Device(s) (SDD) with crypto ignition key(s) (CIK) inserted, passwords, disks and printouts until superseded or downgraded.

3.4. Reporting a Vulnerability or Security Incident/ Violation. AFSSI 5021, *Vulnerability and Incident Reporting*, governs reporting of vulnerabilities or security incidents/violations. Suspect a security incident or violation when there is an unexpected behavior by STARS equipment, the software yields abnormal results (e.g., unexpected output, data spillage or misrouting of data), audit logs indicate unauthorized use or access, unexplained outages, denial of service, loss of accountability, or the presence of a computer virus. Report security incidents involving classified information, including material that resides outside the STARS equipment and software, according to AFI 31-401, *Managing the Information Security Program*.

3.4.1. User node SA/CSSOs will report all STARS security incidents to the STARS SA/CSSO. The Central Node SA/CSSO will begin procedures for a complete assessment including corrective actions or procedures.

3.4.2. The Central Node SA/CSSO will report all security incidents to the STARS System Security Manager (SSM). When notified, the SSM will complete an assessment, including any corrective actions or procedures. Prepare a STARS Security Incident Report (RCS: HAF-XO (AR) 95xx) for the Central Node SA/CSSO. This report is designated emergency status code C-3. Continue reporting during emergency conditions, normal precedence. Submit data requirements in this category as prescribed, or as soon as possible after submission of higher priority reports. Continue reporting during minimize. Provide the following information, as applicable:

3.4.3. Date and time of incident.

3.4.4. Description of incident, such as data spillage, destruction of files, corrupted files, loss of accountability, and other information, which may be pertinent to the investigation.

3.4.5. Impact of the incident.

3.4.6. Corrective action taken, if any.

3.5. STARS Equipment. The Central Node provides, manages, maintains, and exercises configuration control of STARS hardware and software. STARS user node hardware consists of a dedicated personal computer, monitor, keyboard, mouse and SDD with crypto keys. Software consists of commercial, off-the-shelf packages and contractor-developed user node software (UNS). Written authorization must be obtained from the AFCN SA/CSSO prior to making any hardware or software configuration changes.

3.5.1. STARS equipment is owned by and maintained on the AFCN's equipment account. The STARS equipment will not be added to the unit's equipment account.

3.6. Contingencies. The STARS Workbook contains checklist and procedures for manual reporting

3.6.1. Units are responsible for ensuring database is correct upon restoration.

3.7. Access Control.

3.7.1. UserID/Password. If an incorrect UserID and password combination is entered three consecutive times the user account will be locked out. The account will be unusable until unlocked by the user-node SA/ASA. No other user accounts are affected when this occurs.

3.8. User SOP. Users have key responsibilities in operating STARS on a daily basis while maintaining the integrity of the software and to assist in providing the system with the desired degree of security. Responsibility for secure daily STARS operations rests with each user.

3.8.1. Users will:

3.8.1.1. Possess at least a SECRET clearance.

3.8.1.2. Undergo operational and security awareness training prior to using STARS and every six months following certification.

3.8.1.3. Report all STARS security incidents and STARS vulnerabilities to their user node SA/CSSO. Reports containing vulnerabilities or possible vulnerabilities are classified SECRET.

3.8.1.4. Logoff at the end of a work session or for absences longer than five minutes. If the terminal will be out of the user's immediate field of view the user must log off for any absence.

3.8.1.5. Complete a STARS User Password Non-Disclosure Memorandum, which will be provided by your SA/ASA, each time a new password is issued.

3.8.1.6. Ensure data downloaded from STARS is reviewed and marked with the appropriate classification when printed locally.

3.8.1.7. Protect STARS from unauthorized access by using procedures approved by your local DAA and SA/CSSO.

3.8.1.8. Use STARS automated and manual notification checklists when processing notifications.

3.8.1.9. Ensure no classified or sensitive unclassified information can be viewed or accessed by a person who does not meet the security clearance and need-to-know requirements.

3.8.1.10. Protect their password at the appropriate level. Passwords are not to be made available to anyone other than the user and the SA/CSSO. Users must immediately notify their SA/CSSO of any compromise or suspected compromise of a password, or if they forget their password.

3.8.1.11. Notify their SA/CSSO if their password/ user account is no longer required.

3.8.1.12. Remove the CIK and store in an appropriate security container for facilities that do not operate 24 hours a day.

3.8.1.13. Remove the hard drive, as required, and store in the appropriate security container for facilities not operating 24 hours a day.

3.8.2. Users will not:

3.8.2.1. Introduce a malicious code into any STARS equipment.

3.8.2.2. Attempt to bypass, overload or test security mechanisms without written authorization from the Central Node.

3.8.2.3. Import, install, or use unauthorized software or hardware.

3.8.2.4. Violate software copyright or license restrictions.

3.8.2.5. Attempt to gain access to information for which they have no need-to-know.

3.8.2.6. Place food, beverages or any other material on any STARS equipment.

3.8.2.7. Divulge their passwords to anyone.

3.8.2.8. Relocate any part of STARS hardware without specific authorization from the SA/CSSO.

3.9. USER NODE SA/CSSO SOP—General. Wherever SA/CSSO responsibilities are delineated throughout this document, it is implied that the ASA/CSSO holds the same responsibilities in the absence of the SA/CSSO. The SA/CSSO has key responsibilities in overseeing secure operation of their portion of STARS. Overall responsibility for secure day-to-day operation of the unit’s STARS terminal rests with you.

3.9.1. The user node SA/CSSO will:

3.9.1.1. Be appointed, with one alternate, in writing. The original appointment letter will be forwarded to the AFCN SA/CSSO. (See workbook example)

3.9.1.2. Forward original SA Password Non-Disclosure Memorandum to the Central Node to be signed by the STARS Central Node System Administrator. A copy of the memorandum will be sent back to the unit for their records.

3.9.1.3. Request and add user accounts from the Central Node. The SA/CSSO is responsible for conducting a local records checks to identify each individual's clearance, date of clearance, social security number, rank and full name for each account requested. Forward required information to the Central Node SA/CSSO. File copies of password requests or changes are to be maintained for six months per AFMAN 37-139, table 33-25 rule 3. (***NOTE***: The Central Node SA/CSSO will determine whether an individual meets all requirements for access to STARS, and the type of information for which s/he will be granted access. After all requirements are met the Central Node SA/CSSO will issue a UserID/password to the user node SA/CSSO.)

3.9.1.4. Provide UserID/password combination to the authorized user orally. Prepare and retain a password non-disclosure letter for each individual receiving a password, signed by both the user and their supervisor. (See STARS workbook)

3.9.1.5. The SA will sign the non-disclosure letter, certifying that security briefings were given to the user and their supervisor.

3.9.1.6. The Central Node manages all maintenance for STARS-provided equipment as part of the configuration control program. Forward requests for STARS PC or SDD maintenance to the AFCN. Printers, although authorized, are not part of the provided hardware. Any printer connected to STARS is the responsibility of the user node. Ensure the user node MOA is properly executed with the Central Node SA/CSSO.

3.9.1.7. Maintain STARS user node administrative and technical documentation in a single binder. Minimum documentation includes: SA/CSSO appointment letter, the SA Password Non-Disclosure letter (after signature by the AFCN SA), DAA Approval to Process Classified, EMSEC Evaluation/Inspection Results, User Node Accreditation package, and records of security incident/violations or treaty violations. Other documents maintained within the binder must include the SA/CSSO User Node Memorandum of Agreement (MOA), the STARS Self-Inspection checklist, and all equipment receipts.

3.9.1.8. Maintain configuration control over STARS user node hardware, software, and documentation.

3.9.1.9. Report all security incidents and system vulnerabilities involving STARS to the AFCN SA/CSSO.

3.9.1.10. Protect passwords and report any compromise/possible compromise to the Central Node SA/CSSO.

3.9.1.11. Evaluate security, deviations or violations and initiate corrective actions.

3.9.1.12. Complete the accreditation process, and maintain local system accreditation. Each user node will have an EMSEC evaluation performed at their location. Classified EMSEC evaluation results will be stored in a safe, if applicable. Each user node will also complete local requirements for approval to process classified information and be accredited by their local DAA. Copies of the user node accreditation documents and approval to operate will be forwarded to the STARS SA for review and inclusion in the STARS System Security Plan.

3.9.1.13. Attend the 436th USAF STARS Operations Course (Dyess).

3.9.1.14. Train users to operate STARS.

3.9.1.15. Maintain documentation of initial and recurring training.

3.9.1.16. Ensure STARS security requirements are added to existing recurring security training plans. Recurring training is required once every six months as a minimum.

3.9.1.17. No maintenance may be performed on the STARS terminal without authorization from the AFCN. Monitor maintenance activities to ensure that only authorized maintenance is arranged for and performed. Ensure maintenance personnel are properly cleared or escorted.

3.9.1.18. Ensure users are aware as to who is authorized to use STARS.

3.9.1.19. Notify users whenever someone’s authorization to use STARS is revoked. This includes PCA and PCS, or when an individual is determined to be a potential security risk.

3.9.1.20. Delete a user's account from STARS within one workday following a PCS, PCA, loss of clearance, or when a possible or confirmed password compromise occurs.

3.9.1.21. Notify the AFCN when a user no longer requires access to STARS in the performance of assigned duties.

3.9.1.22. The SA will lockout the account of users TDY for more than 10 days. The account will be unlocked upon the users return to duty.

3.9.1.23. Ensure unauthorized personnel are not allowed STARS access and that the controlled area is clearly posted.

3.9.1.24. Conduct a daily audit log review for the following:

3.9.1.24.1. Invalid access attempts

3.9.1.24.2. Accesses to the system on dates or during periods outside of defined operational periods.

3.9.1.24.3. Attempts to use special privileges (e.g., SUPERUSER) for unauthorized activities.

3.9.1.24.4. An abnormal number of aborted access attempts by the same user, or from the same terminal.

3.9.1.24.5. Invalid attempts to access files including READ, WRITE, EXECUTE, and DELETE operations.

3.9.1.24.6. Invalid attempts to access audit log files.

3.9.1.24.7. Attempts to override computer-generated classification markings.

3.9.1.24.8. Attempts to print a file for which a user is not authorized.

3.9.1.25. Backup audit logs to disk or tape weekly.

3.9.1.26. Maintain audit logs and records of the audit log reviews for two years per AFMAN 37-139, table 33-25 rule 8. Appropriate security markings must be on all hardcopy documents and disks/tapes used to store the audit logs.

3.9.1.27. Inspect equipment for signs of tampering such as broken seals or equipment relocation. Perform weekly power on self-tests of the PC equipment and ensure all cables are properly connected.

3.9.1.28. Report audit inconsistencies to the Central Node SA/CSSO if the inconsistency cannot or should not be resolved locally. For example, if the audit shows a user has accessed the user accounts database it should be reported as a security incident/violation.

3.9.1.29. Ensure the PC is configured to boot from the hard drive first.

3.9.1.30. Store the following items so they are accessible to the SA and ASA only:

3.9.1.30.1. STARS software

3.9.1.30.2. SDD master CIK

3.9.1.30.3. Printed or electronic copies of audit logs (Marked and stored as SECRET until reviewed/downgraded)

3.9.1.30.4. Password listings are marked and stored as SECRET. (**NOTE**: A list containing an inventory of all STARS items maintained in a safe is recommended.) An ammo box secured by a combination lock, with the combination known only by the SA and ASA, stored in a GSA approved safe is the preferred storage method. Other methods that provide equal or greater security are permitted.

3.9.1.31. Test emergency procedures and document results as part of the facilities regularly scheduled fire/evacuation drills.

3.9.1.32. The SA/CSSO will forward his/her password non-disclosure letter to the Central Node for signature. All others will be signed by the unit SA and retained locally.

3.9.1.33. Ensure STARS notification processing checklists are available and are being used. (See STARS workbook for samples.)

3.9.1.34. Purge/clear all obsolete computer floppy disks IAW AFSSI-5020, *Remanence Security,* and local procedures.

3.9.1.35. Ensure operators are trained in proper system operation, security and reporting procedures a minimum of once every six months. Include STARS training requirements in the annual training plan and document all training accomplished.

3.9.1.36. Maintain a copy of the START Implementation Policy Guidance Book produced by HQ USAF/XONP and distributed to MAJCOM and Unit CCT'S. This document will be retained until rescinded or incorporated into AFMAN 16-602.

3.9.1.37. Ensure that all STARS users have the screen saver configured as 'Logoff Screen Saver', set to 5 minutes

3.9.2. The SA/CSSO will not:

3.9.2.1. Enter UserIDs/passwords for unauthorized users.

3.9.2.2. Make UserID/passwords available to anyone other than the user and the ASA/CSSO.

3.9.2.3. Make the BIOS password available to anyone other than the ASA/CSSO.

3.9.2.4. Make the STARS software or system emergency recovery disks available to users.

3.9.2.5. Make any changes to the system configuration.

ROBERT H. FOGLESONG, Lt General, USAF
DCS, Air and Space Operations

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 16-601, *Implementation of, and Compliance with, Arms Control Agreements*

AFI 31-401, *Information Security Program Management*

AFI 31-501, *Personnel Security Program Management*

AFMAN 37-139, *Records Disposition Schedule*

AFSSI 5013, *Password Management*

AFSSI 5020, *Remanence Security*

AFSSI 5021, *Computer Security Reporting*

AFSSI 5100, *Air Force Computer Security Program*

OUSD (A)/SAC&C Letter, Subject: Classification of CMTS, 12 Dec 1997

Treaty Between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms (START)

Abbreviations and Acronyms

ACC—Air Combat Command

AETC—Air Education and Training Command

AFMC—Air Force Materiel Command

AFSPC—Air Force Space Command

AMC—Air Mobility Command

ASA—Alternate System Administrator

AUTODIN—Automatic Digital Network

C/E—Conversion/Elimination

CCT/TCO—Treaty Compliance Office

CIK—Crypto Ignition Key

CMTS—Compliance Monitoring Tracking System

CN—Central Node

CSSO—Computer System Security Officer

DAA—Designated Approval Authority

DNA—Defense Nuclear Agency

DOD—Department of Defense

DSN—Defense Switched Network

DTRA—Defense Threat Reduction Agency

EE—Emplacement Equipment

EIF—Entry Into Force

EM—Peacekeeper Emplacers

FOT&E—Follow-on Operational Test and Evaluation

GTM—Ground Training Missile

JCIC—Joint Compliance and Inspection Commission

JS—Joint Staff

LRNA—Long Range Nuclear ALCM

LRNNA—Long Range Non-Nuclear ALCM

MAJCOM—Major Command

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

NLT—Not Later Than

NRRC—Nuclear Risk Reduction Center

NTM—National Technical Means

PC—Personal Computer

SA/CSSO—System Administrator/ Computer System Security Officer

SCDS—START Central Data System

SCUM—STARS Computer Users Manual

SDD—Secure Data Device

SICBM—Small ICBM

SIPRNET—Secret Internet Router Network

SNDV—Strategic Nuclear Delivery Vehicles

SOA—Strategic Offensive Arms

SOP—Standard Operating Procedures

SSP—System Security Plan

ST&E—Security Test and Evaluation

STARS—START Tracking and Reporting System

START—Strategic Arms Reduction Treaty

START II—Strategic Arms Reduction Treaty Two

START III—Strategic Arms Reduction Treaty Three

STU—Secure Telephone Unit

SCUM—STARS Computer Users Manual

SUM—STARS User Manual

TAI—Treaty Accountable Item

TCO/CCT—Treaty Compliance Office

TE—Transport Erector

TLI—Treaty Limited Item

TMOM—Training Model of Missile

UA+TV—Unit Assistance and Training Visit

UN—User Node

USG—United States Government

XONP—HQ USAF/XONP Treaties and Agreements Branch

Terms

Accidental Loss—Any incident that destroys an aircraft or missile to the point that normal elimination procedures cannot be completed (i.e., aircraft lost at sea, explosion or fire).

Air-Launched Cruise Missile (ALCM)—An air launched vehicle designed to deliver a nuclear warhead in an air-to-ground mission. Under START, "ALCM" means an air-to-surface cruise missile of a type, any one of which has been flight-tested from an aircraft or deployed on a bomber after 31 Dec 86.

Category—The classification of heavy bombers in accordance with the START Treaty. There are five classifications of heavy bombers based on their armaments or purpose. ALCM carrier; non-ALCM carrier; non-nuclear; test; and training. ALCM heavy bombers are equipped to carry long-range nuclear ALCMS. Non-ALCM heavy bombers are equipped to carry nuclear weapons other than long-range nuclear ALCMS. Non-nuclear heavy bombers are equipped to carry only non-nuclear weapons. Test heavy bombers are used solely for testing purposes. Training heavy bombers are not equipped to carry weapons, and are used solely to train aircrews.

CCT/TCO—The wing-level START Compliance Office. This office is responsible to the Wing/Unit Commander for all provisions of START to include STARS reporting.

Compliance Monitoring Tracking System (CMTS)—The national-level treaty reporting system of which SCDS and STARS are a part.

Compliance—Act of abiding by the terms and provisions of the START.

Conversion—Changing a strategic weapon from one category to another (e.g., changing an ALCM-equipped B-52G into a training heavy bomber).

Conversion or Elimination Facility—(1) any facility at which strategic weapons are converted from one category to another (e.g., a facility at which an ALCM-equipped heavy bomber is converted into a training heavy bomber) or (2) any facility at which heavy bombers, ICBM's, launch canisters, mobile

ICBM launchers, and first stages of ICBM’s remaining after static testing are disposed.

Designated Approval Authority (DAA)—The individual appointed to accredit a computer system.

Declared Facility—A treaty-accountable facility that is listed in the MOU.

Deployed Heavy Bomber—Any heavy bomber other than a test heavy bomber, a training heavy bomber, or a heavy bomber equipped for non-nuclear armaments; a heavy bomber used for the delivery of nuclear weapons.

Deployed ICBM—Any ICBM that can be contained, or is considered to be contained in a deployed launcher of ICBM’s. (NOTE: An ICBM located at the maintenance facility can be considered to be contained in a deployed launcher if it is of the same type and is still located at the same ICBM base as that launcher and that launcher is empty).

Deployed ICBM and its Associated Launcher—A deployed ICBM and the deployed launchers of ICBM’s that contains, or is considered to contain the deployed ICBM.

Deployed Launcher of ICBM’s—Any silo or mobile launcher other than a test launcher, a training launcher, or a launcher located at a space launch facility, from which an ICBM can be launched.

Disablement Beyond Repair—Any incident that renders a TAI incapable of performing its mission and would not be feasible or cost effective to repair. Normal elimination procedures can be performed (i.e., major structural damage to an aircraft or ICBM motor case).

Distinguishable—Must be obviously different. Refers to differences that can be plainly seen by National Technical Means (NTM) of verification or during an On-Site Inspection (OSI). Obvious differences between Treaty-related items.

Defense Nuclear Agency (DNA)—Located in Alexandria, Virginia, DNA manages the CMTS configuration contract during Research and Development.

Defense Threat Reduction Agency (DTRA)—Founded to monitor the Intermediate-Range Nuclear Forces Treaty. This agency located at Dulles Airport, Washington DC, is responsible for all treaty inspections to include INF, START, CFE, et al.

Entry Into Force (EIF)—The time which a treaty enters into force, with all signatories (parties) being required to comply with its provisions.

Eliminated Facility—A treaty accountable facility which has undergone the required elimination process since EIF.

Elimination—The act of disposing of treaty-accountable items. Heavy bombers must have their tail sections and wings removed, then must be cut in half in order to be considered "eliminated." Excavation or explosion must destroy silo launchers of ICBM’s. Removing the solid propellant and destroying the motor case eliminates an ICBM first stage motor. For elimination of facilities, all strategic offensive arms and support equipment must be removed from the facility, and all silo launcher or fixed structures for mobile launchers must be destroyed.

Emplacement Equipment—Equipment used to put ICBM’s into silo launchers.

Encapsulation—Recording and recovering, but not broadcasting, telemetry data from missile test flights.

Encryption—Altering telemetry data regarding missile flight parameters, so that the data cannot be interpreted if intercepted.

Facility—Any ICBM base, air base, rail garrison, maintenance facility, restricted area, parking site, silo launcher group, ICBM loading facility, production facility, repair facility, storage facility, training facility, conversion or elimination facility, test range, heavy bomber flight test center, space launch facility, or static display site.

Flight test—Launch and flight of a missile to evaluate performance, assess throw-weight, and determine other flight characteristics.

Former Heavy Bomber—A reconnaissance airplane, tanker airplane, or jamming airplane that is not equipped for nuclear armaments or non-nuclear air-to-surface armaments and: (a) that was initially constructed on the basis of the airframe of an existing type of heavy bomber and satisfies the requirements for conversion in accordance with the Conversion or Elimination Protocol; or (b) that has been converted from a heavy bomber in accordance with procedures provided for in the Conversion or Elimination Protocol, or in such a way that it satisfies the requirements for conversion in accordance with the Conversion or Elimination Protocol

Former type—Any type of existing ICBM or SLBM that had been taken out of service before entry into force of treaty (e.g., Minuteman I, A-3 SLBM).

Front section—That part of the final stage of the missile which contains the re-entry vehicle(s), shroud, and (if applicable) penetration aids: the "nosecone" of the missile.

Heavy Bomber (HB)—A bomber aircraft capable of flying over 8000 kilometers or of carrying long-range nuclear ALCMS (e.g., B-1B, B-52, Blackjack, B-2).

Heavy Bomber Equipped for Non-Nuclear Armaments—A non-modern heavy bomber which is not equipped for carrying nuclear armaments.

Heavy Bomber Test Flight Center—A facility other than a heavy bomber production facility at which test heavy bombers, used for testing purposes, are based.

ICBM Base—A facility at which silo launchers for silo-base ICBM's, and one associated maintenance facility, are located.

ICBM Launcher—Any device or platform from which an ICBM can be launched (i.e., silos, Transporter/Erectors Launcher, specially designed rail cars).

Intercontinental Ballistic Missile (ICBM)—A land-based ballistic missile which has a range greater than 5500 kilometers (3600 miles).

Jamming—Interfering with the broadcast of telemetric data.

Joint Compliance and Inspection Commission (JCIC)—A committee with representatives from each party designed to resolve treaty issues.

Joint Staff (JS)—Staff composed of officers from a combination of military services which provides direct support to the Chairman, Joint Chiefs of Staff. Located in the Pentagon, Washington, DC.

Launch Canister—Container in which an ICBM can be transported, stored, and launched.

Launch Weight—Maximum weight of a fully loaded ICBM or SLBM at ignition of first stage; based on data derived from flight-testing.

Long-Range ALCM—An ALCM with a range greater than 600 kilometers (390 miles).

Long-Range Nuclear ALCM (LRNA)—Nuclear-armed ALCM with a range greater than 600 kilometers (390 miles).

Long-Range Non-Nuclear ALCM (LRNNA)—An ALCM with a range greater than 600 kilometers (390 miles) that is not nuclear armed.

Missile Support Equipment—Support equipment for ICBM's includes ICBM Emplacement Equipment (Minuteman Transporter-Erectors and Peacekeeper Emplacers) and training models of missiles (ground training missiles).

Mobile Launcher of ICBM's—Any road or rail launcher from which an ICBM can be launched.

Memorandum of Understanding (MOU)—START contains an MOU on data that lists quantitative and location information about items subject to the treaty; the START database.

New Type—Any type of ICBM or SLBM whose technical characteristics differ from previously declared ICBM's or SLBM's. Differences include: (a) change in number of stages; change in diameter of the first stage greater than five percent, (b) change in throw-weight greater than 21 percent, in conjunction with a change in length of the first stage by 5 percent or more; (c) change in launch weight greater than 10 percent; (d) use of a different type of propellant in any stage; or (e) change in length of assembled missile or first stage by 10 percent or more.

Non-Deployed ICBM—An ICBM which is not in a deployed launcher, nor considered to be in a deployed launcher (e.g., missiles in storage or repair facilities are considered non-deployed ICBM's).

Non-Modern Heavy Bomber—A type of heavy bomber initially based at an air base more than ten years ago.

Notification—The act of one treaty signatory providing the other(s) with information regarding a reportable TAI event.

Nuclear Risk Reduction Center (NRRC)—The Department of State Operations Center, located in Washington, DC, responsible for transmitting treaty notifications to the Other Party (ies).

Nuclear Armaments Other Than Long-Range Nuclear ALCMS—Refers to bomber weapons other than long-range nuclear ALCMS (i.e., short-range attack missiles (SRAM's), gravity bombs).

Operational Test & Evaluation (OT&E)—Testing and evaluation conducted in as realistic an operational environment as possible to estimate the prospective system's military utility, operational effectiveness, and operational suitability. In addition, OT&E provides information on organization, personnel requirements, doctrine, and tactics. Also, it may provide data to support or verify material in operating instructions, publications, and handbooks. Under START, "OT&E" refers to the testing of operational (deployed) strategic weapons systems (e.g., an ICBM removed from a deployed launcher and taken to Vandenberg AFB for launch).

Payload—The warhead, its container, and activating devices in a military missile. Under START, "payload" is defined as, for a stage. All that separates from that stage, excluding the front section shroud and the propellant burned by that stage, beginning at the time when the velocity of the final stage is equal to 1,000 meters per second less than its velocity at the time of termination of main engine thrust of the final stage or at the time of the first release of a reentry vehicle or penetration aid, whichever occurs first. The reentry vehicles (warheads) and any penetration aids carried by the missile.

Penetration Aids—Techniques and/or devices employed by offensive aerospace weapon systems to increase the probability of penetration of enemy defenses.

Procedures for Dispensing Reentry Vehicles—The in-flight maneuver by which reentry vehicles are positioned and separated from the Post Boost Vehicle of the missile and directed to individual targets.

Production Facility—Site at which ICBM's that are transported as complete missiles are assembled; where first stages of ICBM's that are maintained, stored and transported in stages are assembled; and where heavy bombers are built.

Prototype—A new type of ICBM which is not yet subject to the numerical limitations of START treaty Article II. Unless its development is canceled, an ICBM is no longer considered a prototype. It becomes subject to the numerical limitations of Article II of the Treaty when one of the following occurs: (1) it is declared to carry a specific number of warheads and to have a specific throw-weight; (2) the 21st prototype is flight-tested; or (3) a launcher for the prototype is deployed.

Range—Maximum distance that an ICBM or ALCM is capable of traveling. Maximum distances that a heavy bomber can fly with a full load of weapons without refueling.

Reentry Vehicle—That part of a space vehicle designed to re-enter the Earth's atmosphere in the terminal portion of its trajectory. Under START, "reentry vehicle" means that part of the front section that can survive reentry through the dense layers of the Earth's atmosphere and that is designed for delivering a weapon to a target or for testing such a delivery.

Repair Facility—A site located outside an air base, or ICBM base, whose role is the repair and maintenance of ICBM's, and heavy bombers.

Residual Propellant—The amount of propellant that is unusable or remains unused in each stage of a missile after its flight.

STARS SA/CSSO—Individual appointed by HQ USAF/XONP responsible for operation and monitoring of the USAF STARS system.

Retired Type—A type of ICBM, which was deployed at the time of START EIF but subsequently taken out of deployment.

START Central Data System (SCDS)—The national-level START reporting system. The USAF STARS Central Node transmits Air Force notifications into SCDS.

Secure Data Device (SDD)—Similar to a STU-III without a hand set, this modem is designed to transmit data high speed in a secure mode. STARS require the AT&T models 1900 and/or 1910 SDDs.

Self-Contained Dispensing Mechanism—A device that separates from the final stage of a missile then targets and releases re-entry vehicles toward their targets.

Silo Launcher for ICBM's—A fixed, in-ground silo structure from which ICBM's can be launched.

Silo Training Launcher—A silo launcher used to train.

Strategic Offensive Arms (SOA)—ICBM's, SLBM's, and heavy bombers.

Soft-Site Launcher—Any fixed, land-base launch site that is not located in a silo; a launch site that is not "hardened" to withstand nuclear blast effects.

Solid Rocket Motor—Part of the missile, which contains solid fuel for propulsion.

Space Launch Facility—Specified site from which satellites and other objects are put into the upper atmosphere or space, using ICBM or SLBM as launch platforms.

Specified Facility—A facility declared in the START MOU.

Stage—A self-propelled section of an ICBM capable of giving its payload an additional velocity of more than 1,000 meters per second.

STARS—START Tracking and Reporting System

Strategic Arms Reduction Treaty (START)—Treaty between the United States of America and the Union of Soviet Socialist Republics on the Reduction and Limitation of Strategic Offensive Arms. START was signed in Moscow on 31 July 1991 and entered into force on 5 December 1994.

Storage Facility—A specified location outside an ICBM base, air base, test range, or space launch facility where ICBM's, or heavy bombers are stored.

Secure Telephone Unit (STU-III)—Allows for secure communications via voice or data encryption.

Treaty Accountable Item (TAI)—A general term used to describe items contained in the treaty (e.g., heavy bombers, ICBM's, mobile ICBM's, and ICBM support equipment).

Transporter Erector (TE)—Any vehicle which can transport a missile and raise or lower it into a launcher.

Telemetric Information—Data broadcast or recorded from a missile resulting from a flight test; the data concerns the missile's performance and flight characteristics.

Test Launcher—ICBM launcher located at a test range, from which missiles are launched for flight tests.

Test Range—Designated land area outside of an ICBM base where flight test are conducted.

Throw-Weight—The maximum weight that a missile is capable of carrying over a certain range.

Treaty Limited Item—Any item on which numerical limits have been placed by the Treaty (e.g., warheads, ICBM's, ICBM Launchers, SLBM's, and heavy bombers).

Training Heavy Bomber—A heavy bomber used to train; the bomber is not equipped for nuclear or non-nuclear weapons, and must be based at a designated training facility for heavy bombers.

Transport-Loader—A vehicle capable of moving a fully assembled mobile ICBM from one place to another, and subsequently loading it onto, or unloading it from, a mobile ICBM launcher.

Variant—A classification of heavy bombers of one type or category that are noticeably different from other aircraft of the same type and category (e.g., Turbojet engines on B52G and the Turbofan engines on B52H are visibly distinguishable). Also a classification of ICBM's of one type that are noticeably different from other missiles of the same type or a classification of ALCM's of one type that are distinguishable from ALCM's of the same type.

Verification—The process of judging information gathered about the practices of a party to a treaty in order to evaluate whether the party is adhering to the terms and provisions of the treaty.

Version—For mobile launchers of ICBM's, and for fixed structures and support equipment of such launchers, a classification based on distinguishable differences from other mobile launchers, fixed structures, and support equipment of the same type of ICBM's.

XONP—Treaties and Agreements Branch, HQ USAF/XONP.

Warhead—That part of a missile, projectile, torpedo, rocket, or other munitions which contains either the nuclear or thermonuclear system, high explosive system, chemical or biological agents or inert materials intended to inflict damage. Under START, “warhead” means a unit of account used for counting toward the 6000 maximum aggregate limit and relevant sub limits as applied to deployed ICBM’s, deployed SLBM’s, and deployed heavy bombers.