BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-107, VOLUME 1

1 SEPTEMBER 1997

Communications and Information

STRATEGIC AUTOMATED COMMAND CONTROL SYSTEM-DATA TRANSMISSION SUBSYSTEM (SACCS-DTS) SOFTWARE CONFIGURATION MANAGEMENT AND CHANGE CONTROL

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFSPC/SCMB
(Mr Norman Schwiesow)

Certified by: HQ USAF/SCXX
(Lt Col Francis X. McGovern)
Pages: 16
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*. It prescribes the requirements, responsibilities, and procedures for operation, security, and configuration management of the Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS). It applies to all users of the SACCS-DTS Network, either through direct input or interface systems. When major commands (MAJCOMs) and field operating agencies (FOAs) supplement this instruction, they should provide a copy to Headquarters Air Force Space Command (HQ AFSPC)/SCMB, 150 Vandenberg Street, Ste 1105, Peterson AFB CO 80914-4730, with a copy to Headquarters Air Force Communications Agency (HQ AFCA)/XPXP, 203 W. Losey Street, Room 1065, Scott AFB IL 62225-5224. Refer recommended changes and conflicts between this and other publications to HQ AFSPC/SCMB, using AF Form 847, **Recommendation for Change of Publication,** with an information copy to HQ AFCA/XPXP. See **Attachment 1** for a glossary of references, abbreviations, an acronyms.

1. Terminology and References.

1.1. Applicability**.** This instruction applies to all users who either interface with or support the Strategic Automated Command Control System, Data Transmission Subsystem (SACCS-DTS) Network. The SACCS-DTS Network provides commanders with information required for decisions affecting the control and direction of strategic forces. In addition, it provides subscribers with direct interface to the Automatic Digital Network (AUTODIN), Air Force Global Weather Center (AFGWC), Command Center Processing and Display System (CCPDS), and at Peacekeeper Intercontinental Ballistic Missile sites with Air Force Satellite Communications System (AFSATCOM), and Survivable Low

Report Documentation Page

Report Date 01 Sep 1997	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Air Force Instruction 33-107, V1, Communications and Information, Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Software Configuration Management and Change Control	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Pentagon Washington, DC 20330-1250	**Performing Organization Report Number** AFI33-107V1
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 16	

Frequency Communications System (SLFCS). SACCS is two major electronically interconnected subsystems; the DTS and the Data Processing Subsystem (DPS).

1.2. Authority And Organization**.** HQ AFSPC, as the lead command of the SACCS-DTS Network, is responsible for the operations, hardware maintenance, and software maintenance. They also provide operational guidance and hardware support. As the system program manager for acquisition , HQ Air Force Materiel Command (SM-ALC/LHO), provides service support according to DoD-STD-5000, *Defense Acquisition;* and Department of Defense (DoD) Directive 5000.1, *Defense Acquisition*, March 15, 1996. The 55th Computer Systems Squadron (55 CSS), 55th Wing, Air Combat Command (ACC), Offutt AFB NE, provides operational and software support through the Computer Program Maintenance Facility (CPMF) and SACCS Operations Facility. Configuration management and software change control are the responsibility of the commander, 55 CSS, and the network software functional manager (NSFM).

1.3. Terminology.

1.3.1. Change Classification**.** A method of grouping system changes according to their nature, magnitude, and effect. Each group requires slightly different processing and reviewing procedures. Changes to system software, hardware, procedures, or documentation fall into one of two categories:

1.3.1.1. Class I Change. A major modification or new capability to software programs. The Design Control Board (DCB) reviews all requirements and discrepancies designated as Class I changes, whether software, hardware, or procedural. Submit Class I changes on a Baseline Change Request (BCR) form.

1.3.1.2. Class II Change. A deficiency, discrepancy, or problem that typically requires a minor correction to documentation or software to comply with existing requirements. Submit Class II changes on a Software Problem Report (SPR) form or on AF Form 1067, **Modification Proposal**. The Requirements Analysis Team (RAT) monitors and approves Class II changes.

1.4. References**.** See **Attachment 1**.

1.5. Document Responsibility**.** The commander, 55th Computer Systems Squadron, is the office of collateral responsibility for this instruction. Address questions to:

55 CSS/CMTQ

201 Lincoln Highway, Suite 206

Offutt AFB, NE 68113-2040

2. Software Problem Reporting.

2.1. Software Review Bodies**.** The following bodies handle the review, approval, and management of software change requests.

2.1.1. Design Control Board (DCB). This board includes highly qualified members from software development, plans and management, and user communities.

2.1.1.1. Reviews and approves all proposed Class I change requests.

2.1.1.2. Advises the designated approval authority (DAA) on the review and actions taken for all Class I changes.

2.1.1.3. Forwards all approved changes to the Requirement Analysis Team (RAT) for action.

2.1.2. RAT. This team is the management and review body at the CPMF level.

2.1.2.1. Reviews Class II change requests for approval, and accepts Class I change requests from the DCB.

2.1.2.2. Plans the specific programming actions for the change and monitors its progress through the software development cycle.

2.2. Requesting Changes**.** Any SACCS-DTS user can submit change requests. Submit the change request to 55 CSS/CMT by letter or message through the SACCS-DTS Network Quality Control Center (NQCC). You can also use AF Form 1067. Report operational discrepancies (computer aborts, hardware and or software problems) directly to the NQCC.

2.3. Normal Problem/Trouble Reporting. The NQCC provides near real-time status of the entire SACCS-DTS Network. The NQCC maintains records of all outages, downtimes, discrepancies, and corrective actions through the SACCS Trouble Monitor Report (STMR).

2.3.1. SACCS-DTS software provides automatic reporting of Initial Program Loads (IPLs), restarts, line outages, and equipment failures to the NQCC. Node operators provide any additional information requested by NQCC.

2.3.2. Facts pertaining to specific problems (user isolations, equipment failures, line outages, etc.) are not classified, unless analysis determines a threat to the entire network. The Network Security Manager makes the classification determination, using the SACCS-DTS Classification Guide.

2.3.3. To report a problem in system performance, users must notify NQCC by message to SACCS-DTS address SACNC. Use any format, but include the following information:

2.3.3.1. SACCS-DTS address of processor or Collocated User Terminal Element (CUTE) where problem occurred.

2.3.3.2. Date/Zulu Time Group of problem.

2.3.3.3. Name and duty phone of person(s) to contact regarding the problem.

2.3.3.4. Software version in use (available on Initial Program Load (IPL) diskette label).

2.3.3.5. A free text description of actions leading to the problem, how the system failed, and corrective measures taken.

2.3.3.6. The dump diskette label identification (ID) number, as applicable.

2.3.4. For unusual occurrences (those not normally reported as discrepancies or disruptions), generate a letter or message immediately to the NQCC. The report should include:

2.3.4.1. Circumstances of the occurrence, including down and up times.

2.3.4.2. The site, terminal, or functional area (FA) where the problem occurred.

2.3.4.3. Applicable hardware registers, and any dump(s) taken.

2.3.4.4. Any other pertinent information.

2.4. Documentation. All computer systems and programs require written documentation, with supporting references, to function successfully. Documentation must satisfy the needs of programmers, analysts, operators, and management personnel. The four categories are:

2.4.1. Application documentation. Provides programmers, testers, and configuration management personnel the ability to ensure the integrity and operability of all code segments. Application documentation includes:

2.4.1.1. System documentation describes the interrelationship of the system and its various programs and subprograms. System documentation also describes the interrelationship of the system and program with any related resources and references.

2.4.1.2. Program documentation describes the logic of the program flow in narrative form, to aid the programmer in understanding what the program is accomplishing.

2.4.1.3. Computer source code printouts describe the program operation, including comments to support program maintenance, debugging, and modification.

2.4.2. Operator documentation. Operators and other system users require documentation that provides instructions for man-machine interaction. User's guide, or system notification message listings are examples of operator documentation.

2.4.3. Maintenance documentation. Maintenance personnel require documentation to maintain the system and diagnose fault areas. This includes hardware and software diagnostics, abort lists, error codes, unique procedures and software associated with special tests.

2.4.4. Management documentation. Management personnel require a general, but well-defined narrative of major programs, sub-programs, and sub-routines as they function in the system. This provides command-level management the knowledge necessary to make decisions on system operations and software changes.

2.5. Program Testing. The objective of program testing is to increase confidence that the software functions as intended in the operational environment and that it meets all specified requirements.

2.5.1. Test and document all software changes before configuring and authorizing release as operational software.

2.5.2. Test system software in an environment that represents its normal operational configuration to the fullest extent possible.

2.5.3. Document software and testing results at the appropriate level.

3. Configuration Management.

3.1. General. This paragraph establishes procedures for configuring and controlling SACCS-DTS software. All SACCS functions must:

3.1.1. Design, test, document, coordinate, and disseminate all software changes in an orderly and controlled manner. Incorporate only approved and configured software changes into current operational, utility, support and maintenance software.

3.1.2. Assign a unique control number for all software products and changes. Use the project control number to identify each line of code added or modified as a part of the project. SACCS

Configuration Management maintains the control numbers and establishes the baseline for diskette content.

3.2. SACCS Configuration Management (55 CSS/CMTQ):

3.2.1. Maintains a master program library of the current and last two superseded source code listings on tape for each computer program release.

3.2.2. Maintains each baseline listing (major release) until no longer needed.

3.2.3. For on-line operational programs, retains a printed text listing of the master copy of the current operational software.

3.2.4. Promotes and configures all completed projects for release and develop a release plan. Develops golden master diskettes for the operational librarian (55 CSS/CMOL) to use in release production.

3.2.5. Does not implement any changes that impact missile operations until technical orders and operational manuals reflect the change.

3.3. Release Implementation**.** Controls release and distribution of software upgrades to prevent the possibility of unauthorized modification (see **Attachment 4**). There are three types of software release implementations.

3.3.1. Major Release. A major release generally applies to a release affecting all sites in the SACCS-DTS Network. Identify major releases by the first letter of the Version ID and seven zeros (e.g., A0000000). Implementation may be incremental or simultaneous. For an incremental implementation, the existing software must work with the new software. Distribute a Software Version Description (SVD) detailing the changes made in the new release in conjunction with the software.

3.3.2. Interim Release. Occasionally, it is necessary to correct software deficiencies or implement operational requirements on an interim basis before the next scheduled major release. Interim releases are identified by alphabetic characters in the fifth and sixth positions of the Version ID (e.g., A000*aa*00). After building the interim software for affected nodes in the network, implement by one of these methods:

3.3.2.1. Electronic Program Update (EPU) (see **Attachment 1**). Update software at affected nodes. This will eliminate the need to generate and distribute IPL diskettes and a SVD. Do not employ EPU for any changes involving Trusted Computing Base (TCB).

3.3.2.2. Normal Release Distribution. Prepare and distribute IPL diskettes in the same manner as a major release, including a SVD.

3.3.3. Emergency Release. When the nature of a software or operational issue requires an immediate change, prepare an emergency release. Identify emergency releases by entering numbers in the last two character positions of the Version ID (e.g., A00000*nn*). Limit emergency releases to single changes when possible. Since it bypasses normal software configuration procedures, use emergency releases with caution. Incorporate all emergency release changes in the next interim or major release (if still in effect). Implement emergency releases in the same manner as a major release. Substitute a Release Implementation Plan (RIP) for the SVD.

3.4. Diskette Handling. Maintain software and operational information for the SACCS-DTS on eight-inch diskettes. Verify the integrity of the shipment by inspection of the SACCS-DTS blue logo tape (see **Attachment 5** for inspection procedures). Label each software diskette with the applicable configuration control designation and identifying data (i.e., release version, site, and date created).

3.4.1. Handling. Protect the diskettes from extreme temperatures, magnetic forces, bending, and contaminants. Do not touch exposed surfaces on the diskette. When storing diskettes, keep the diskette in the protective jacket when not in the disk drive. Failure to follow these instructions could lead to damaged media.

3.4.2. Diskette Classification. Once placed in the processor, classify and control **ALL** diskettes at the security level of the processor. Regardless of classification, account for all diskettes. Units will implement local procedures to account for UNCLASSIFIED and SECRET diskettes. Account for TOP SECRET diskettes according to DoD Regulation 5200.1, *DoD Information Security Program Regulation*, June 1986, with Changes 1 and 2, and AFI 31-401, *Managing the Information Security Program*.

3.4.2.1. IPL Diskettes: IPL diskettes are UNCLASSIFIED when shipped from 55 CSS/CMOL (SACCS Library). Retain IPL diskettes as directed by the current Version Description Document, paragraph 2.6. Package and store superseded release versions at a separate location to prevent inadvertent use. Destroy all other IPL diskettes according to paragraph **3.4.7.**

3.4.2.2. System Diskettes (Menu, Journal, Dump, Empty): System diskettes are UNCLASSIFIED when shipped from 55 CSS/CMOL (SACCS Library). Retain diskettes for reuse within the same processor until the diskette is unusable. Once unusable, destroy the diskette according to paragraph **3.4.7.**

3.4.2.3. Diagnostics Diskettes. Diagnostic diskettes are formatted with specific files. System configuration and file structure prevent them from containing any information higher than UNCLASSIFIED/For Official Use Only (FOUO). Employ and store diagnostic diskettes according to operations requirements and local procedures. Unusable or obsolete diskettes should be destroyed according to paragraph **3.4.7.**

3.4.3. The SACCS Operational Librarian (55 CSS/CMOL):

3.4.3.1. Maintains an emergency back-up set of master diskettes for the current and the latest superseded software versions. Stores back-up masters off-site for back-up integrity.

3.4.3.2. Produces release software diskettes. Distributes release diskettes with the SVD or RIP. Distributes new software versions only to those sites requiring the changes.

3.4.3.3. Uses US Postal Service, Registered mail or United Parcel Service (UPS) to distribute outgoing IPL diskettes. Seals the inner wrapping with logo tape imprinted with the SACCS-DTS logo.

3.4.3.4. Does not use software master diskettes for any purpose other than for reference and emergency reproduction.

3.4.4. Diskette Retention.

3.4.4.1. Dump Diskettes. Retain used dump diskettes for a minimum of 10 days. If not required for dump analysis, reuse dump diskettes as necessary.

3.4.4.2. Journal Diskettes. Base Communications Processors (BCPs) retain journal diskettes for 10 days. SCPs retain journal diskettes for 30 days. If not required for system analysis or message tracking, reuse journal diskettes as necessary.

3.4.5. Diskette Analysis. If there is a need to analyze a dump diskette or journal diskette, NQCC will arrange remote dump action and or shipment of the diskette. Missile crews will not process remote dump actions from the Launch Control Centers (LCCs), but return dump diskettes to the issuing agency for remote dump processing. When shipping diskettes, comply with the requirements of DoD Regulation 5200.1 and AFI 31-401 for handling classified media.

3.4.6. Diskette Labeling. Reference AFI 33-107, Volume 2, *Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Network Security Program* (**Attachment 2**) for specific labeling instructions. The 55 CSS/CMO labels diskettes with identifying serial numbers and a diskette name. Do not remove this label. Label each diskette with markings or warning notices (i.e., Restricted Data, Single Integrated Operational Plan (SIOP), etc.) accordingly. Do not remove United States Strategic Command (USSTRATCOM) Form 148, SIOP Label, once placed on the diskette.

3.4.7. Diskette Destruction.

3.4.7.1. Destroy classified media according to Air Force System Security Instruction (AFSSI) 5020, *Remanence Security*. **NOTE:** Destroy the diskettes locally. Do NOT return media to SACCS Library for destruction.

3.4.7.2. Document destruction of diskettes according to DoD Regulation 5200.1 and AFI 31-401. Forward one information copy of destruction records to the 55 CSS/CMOL (SACCS Library) for accountability purposes.

4. Configuration Management Responsibilities.

4.1. DAA. HQ AFSPC, as the lead command of the SACCS-DTS Network, is the DAA. The responsible office is HQ AFSPC/SCX (Plans and Programs). Their responsibility includes all operational, configuration, and security issues impacting the SACCS-DTS Network either through direct processing or interface with other systems.

4.2. MAJCOMS. Other MAJCOMs using the SACCS-DTS Network will comply with the requirements of this instruction. Each MAJCOM will designate an action officer to act as a point of contact (POC) for SACCS users within their command. Notify HQ AFSPC/SCX and SACCS/NSM of SACCS POCs.

4.3. Network Operations**.** The commander, 55 CSS, is responsible for the overall operation and configuration management of the SACCS-DTS Network, including operation and management of the CPMF.

4.4. NSFM. The commander, C2 Systems Flight (55 CSS/CMT), will serve as the NSFM. Through sound configuration management, the NSFM will ensure responsiveness and integrity of the software for the SACCS-DTS Network. The NSFM will:

4.4.1. Direct the activities of programming personnel engaged in design, development, production, documentation, and control of all operational, utility and analysis programs. This includes day-to-day resolution of program deficiencies and production procedures to meet current and future operational requirements.

4.4.2. Evaluate, develop, design, and implement current and future communications concepts and requirements that affect DTS programming activities.

4.4.3. Advise system users on present and future software requirements.

4.4.4. Thoroughly test all software programs before implementation.

4.4.5. Ensure programmers and testers remain qualified to maintain software changes.

4.5. The commander, SACCS-DTS Operations Flight (55 CSS/CMO):

4.5.1. Supports implementation and operation of software releases.

4.5.2. Ensures operational hardware and computer program configuration, at all locations, through the SACCS NQCC at Offutt Subnet Communications Processor (SCP). The NQCC acts as a 24 hour focal point and information distribution center for the network and the AFSPC Senior Communications-Information Systems Officer (CSO). The Operations Flight provides network status, problem reports, and related information to the CMT Flight Commander.

4.5.3. Configures systems and verifies operation to support data dump, journal analysis, and system test operations.

4.5.4. Supports Software Requirements and Configuration Management through operation of CPMF systems and functions.

4.5.5. Maintains system diskettes and tape libraries in support of Operational, Host, and STF operations.

4.6. Officer In Charge (OIC), SACCS-DTS SCP. Each OIC of a SACCS SCP is directly responsible to the AFSPC Senior CSO as follows:

4.6.1. Ensures personnel are proficient in computer operations and in the use of operational, utility, and support software.

4.6.2. Implements all DTS software releases except for maintenance programs.

4.6.3. Supports special operational requirements and tests as directed by HQ AFSPC/DOO (Director of Current Operations).

4.7. OIC, SACCS-DTS Functional Areas: The OIC of each unit or office with a SACCS-DTS FA:

4.7.1. Ensures all personnel are proficient in the operation of SACCS functional area equipment.

4.7.2. Immediately reports problems and necessary system changes to minimize impact on SACCS-DTS Network operations. This includes support of NQCC operations in resolution of on-line network problems when such support does not interfere with operational mission requirements.

4.8. Network Operations Personnel**.** Network operations personnel operate the primary SCP at Offutt Air Force Base. Duty positions include:

4.8.1. Message Service Center (MSC) Operator (Offutt SCP only). The MSC Operator monitors the MSC terminal and associated printer for system and user generated notifications. These notifications indicate potential impacts to the security and integrity of network operations. The MSC Operator will report any network problems to the commander, SACCS-DTS Operations (55 CSS/CMO), provide periodic updates, and initiate appropriate corrective action.

4.8.2. NQCC Operator (Offutt SCP only). The NQCC Operator monitors indications of network problems, either hardware or software. The NQCC Operator reports any network problems on the STMR. The NQCC Operator also compiles notification statistics, and provides any necessary historical data to support problem investigation and resolution. When network connections fail with the missile LCCs, the NQCC requests restoration assistance from the appropriate Wing/Group Communications Job Control.

4.8.3. Switch Operator Position (SWOP) Operator. The SWOP Operator monitors the SWOP for indication of functional area problems, and reports any occurrence to NQCC. At the direction of NQCC, the SWOP performs actions necessary to restore access to the network.

4.9. Hardware And Firmware Support Personnel**.** Hardware and firmware support personnel includes everyone involved with acquisition, maintenance, upgrade, and replacement of SACCS-DTS hardware. All maintenance personnel must comply with configuration management and requirements to maintain network integrity. The primary responsibility for hardware/firmware management rests with the SACCS Program Manager. Local responsibility is delegated to the Network Hardware Functional Manager (NHFM) at each functional area.

4.9.1. Network Hardware Functional Manager: The senior maintenance technician at each SACCS FA will serve as the NHFM. The NHFM:

4.9.1.1. Notifies NQCC of all hardware modifications and upgrades prior to initiating maintenance actions.

4.9.1.2. Ensures all hardware identified for removal from the system is properly purged and declassified.

4.10. Network And System Users. A network or system user is any individual using the SACCS-DTS Network to transmit or receive messages, either through direct terminal or through interface systems.

4.10.1. Network users must comply with the network security plan and local security procedures. All users must immediately report network problems to the NQCC.

4.10.2. Interface users must comply with configuration management requirements as stated in memorandums of agreement between the interface systems and the SACCS-DTS Network. Report upcoming changes and modifications to the interfaced system according to interface memorandums of agreement.

4.11. Software Support Personnel**.** All SACCS-DTS programmers, systems analysts, and configuration management personnel will support configuration management and change control. All software support personnel will support the NSFM and Network Software Security Officer **(**NSSO) in development, maintenance, and configuration management of SACCS-DTS software.

4.12. NSSO. The commander, 55 CSS appoints the NSSO. The NSSO must know the SACCS-DTS security policy. The NSSO must have a thorough understanding of the TCB software and the TCB relation to security policy implementation. The NSSO must also be well versed in computer security and familiar with formal verification tools. The NSSO:

4.12.1. Formally verifies SACCS-DTS software. Accomplish this verification before each certification and accreditation of the network, or as directed by the DAA. Maintain the formal top level specifications.

4.12.2. Compares software design specifications to written source code to verify correlation between them.

4.12.3. Performs a software penetration test before each certification and accreditation cycle, or as directed by the DAA.

4.12.4. Assists programmers and configuration managers during the software development process.

4.12.4.1. Provides security input and recommendations to the RAT for the initial evaluation of software change projects.

4.12.4.2. Provides security input and recommendations to the programming team during the design review.

4.12.4.3. Reviews the Documentation Change Request for security requirements and completeness.

4.12.4.4. Conducts a Trusted Code Review for all projects involving trusted code before building diskettes for each software release. Documents and maintains the review, with copies of the applicable source units.

WILLIAM J. DONAHUE, Lt General, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, AND ACRONYMS

References

DoD Regulation, *DoD Information Security Program*

DoD Directive 5000.1, *Defense Acquisition*

DoD-STD-5000, *Defense Acquisition*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFI 31-401, *Managing the Information Security Program*

AFI 33-107, Volume 2*, Strategic Automated Command Control System-Data Transmission Subsystem (SACCS-DTS) Network Security Program*

Abbreviations and Acronyms

AFSPC—Air Force Space Command

CPMF—Computer Program Maintenance Facility

CSS—Computer Systems Squadron

DAA—Designated Approval Authority

DCB—Design Control Board

DTS—Data Transmission Subsystem

EPU—Electronic Program Update

FA—Functional Area

FOUO—For Official Use Only

ID—Identification

IPL—Initial Program Load

MSC—Message Service Center

NHFM—Network Hardware Functional Manager

NQCC—Network Quality Control Center

NSFM—Network Software Functional Manager

NSSO—Network Software Security Officer

RAT—Requirements Analysis Team

RIP—Release Implementation Plan

SACCS—Strategic Automated Command Control System

SCP—Subnet Communications Processor (Accountable Processor)

SIOP—Single Integrated Operational Plan

STMR—SACCS Trouble Monitor Report

SVD—Software Version Description (formerly known as the VDD)

SWOP—Switch Operating Position

TCB—Trusted Computing Base

Attachment 2

SAMPLE CHANGE REQUEST MESSAGE
(FOUO WHEN FILLED IN)

Prepare change request message as follows:

UNCLASSIFIED/NOCAT/JJ

P TO SACMC/PASS TO 55CSS/CMT//INFO SACFS//(stx)

UNCLASSIFIED JOREP JIFFY __________ SACCS CHANGE MESSAGE.

ORIGINATOR: _________PHONE: ________ORGANIZATION: ___________

DATE: _____________TIME: ______________Z SOFTWARE RELEASE:

PROBLEM/ENHANCEMENT DESCRIPTION (if applicable):

DUMP DISKETTE LABEL ID# ______________

PSW _____ IAR _____ AKR _____ LSR _____

R0 _____ R1 _____ R2 _____ R3 _____ R4 _____ R5 _____ R6 _____ R7 _____
(from SWOP after a restart)

Explain in as much detail as possible the desired enhancement or the desired change. Describe the advantage or impact this change will provide in work hours or dollars, and its operational requirement.

Attachment 3

EPU ADVISORY MESSAGE FORMAT

Prepare EPU advisory message as follows:

CLASSIFICATION/NOCAT/JJ.

R TO: Addresses of functional areas that will receive the EPU. Include any Info address to make other organizations aware of the activity.

GENERAL: Notification that specified FAs will receive operational software changes through the EPU process. This paragraph will also address shipment of new diskettes and any additional EPUs planned in support of this software change.

PURPOSE: A brief justification of the change, and the impact/detail of the change on affected FAs.

IMPLEMENTATION INSTRUCTIONS: Technique or procedures on how to implement software and other unique information for a specific type of functional area. Include:

CRC Key and proposed transmission time.

New software version identification.

Specific instructions and diskette write/enable requirements.

VERIFICATION INSTRUCTIONS: Guidance on what to observe to confirm proper implementation.

FALLBACK GUIDANCE: Instructions on what to do if the software update fails.

SUPERSEDED DISKETTE DISPOSITION: What to do with the old diskettes.

IMPLEMENTATION COORDINATOR: Name, office symbol, office phone, non-duty hour point of contact, message address.

TIME: List of nodes and the scheduled time for the EPU process. The actual time for the IPL of the new software, if other than immediate implementation. Remember to refer to the SACCS Classification Guide for classification requirements on software release implementation.

CONTINGENCY INSTRUCTIONS: What to do if unable to support the EPU at the scheduled time.

Attachment 4

SAMPLE RELEASE IMPLEMENTATION MESSAGE

Prepare release implementation message as follows:

(CLASSIFICATION)/NOCAT/JJ

O TO: (Address of functional areas required to implement the scheduled release. Include information addresses to make other organizations aware of the activity.)

(CLASSIFICATION) JOREP JIFFY ______SACCS SOFTWARE RELEASE (version) IMPLEMENTATION

PLEASE PASS A COPY OF THIS MESSAGE TO YOUR MAINTENANCE SUPPORT ORGANIZATION.

THE IMPLEMENTATION OF SACCS SOFTWARE RELEASE (version) WILL TAKE PLACE COMMENCING dd mm yyyy, AT hhmmZ. IMPLEMENT RELEASE (VERSION) USING THE RELEASE IMPLEMENTATION PROCEDURES CONTAINED IN SECTION 2.4. OF THE SVD SHIPPED WITH EACH DISKETTE PACKAGE AND THE SCHEDULE LISTED BELOW. PLEASE READ THE ADDENDUM IN THE FRONT OF THE SVD. THIS IMPLEMENTATION INCLUDES (types, and/or list of nodes affected)

DIRECT QUESTIONS REGARDING THE IMPLEMENTATION SCHEDULE TO 55 CSS/CMTQ DSN 271-7150/2462 OR VIA SACCS ADDRESS “SACMC/ATTN CONFIG MANAGEMENT//."

PHASE THE (version) IMPLEMENTATION FOR MINIMUM DISRUPTION TO SERVICE WITHIN THE NETWORK. EACH GROUP LISTED BELOW WILL PERFORM THEIR IPL AT THE SPECIFIED TIME USING THE APPROPRIATE PROCEDURES IN THE SVD. ANY SITE LISTED BELOW THAT IS UNABLE TO IPL AT THEIR DESIGNATED TIME WILL IPL WITH THE NEW SOFTWARE AS SOON AS THEY REGAIN IPL CAPABILITY:

GROUP 1 = base - processor, base - processor, base - processor

hhmmZ   base - processor.

GROUP 2 = base - processor, base - processor, base - processor

hhmmZ   base - processor.

GROUP 3 = base - processor, base - processor, base - processor

hhmmZ   base - processor.

THIS IS A COORDINATED AFSPC/625 MOF/SACCS, 55 CSS MESSAGE.

TTYADD: TO:
INFO:

DECLASS: (OADR) 48 HOURS AFTER IMPLEMENTATION.

Attachment 5

BLUE LOGO TAPE INSPECTION PROCEDURES

A5.1. General. The tape is 3 5/8” wide and composed of three layers; an adhesive layer, a fiber layer, and a paper layer. The paper layer is blue with the SACCS-DTS logo imprinted with red ink.

A5.2. Inspection Procedures.

A5.2.1. Verify the blue logo tape is used only to seal the inner wrapping.

A5.2.2. Check for tampering.

A5.2.2.1. Check for the presence of the unique SACCS-DTS logo design.

A5.2.2.2. Check for signs of de-lamination or separation of the tape layers.

A5.2.2.3. Check for signs of discoloration or staining. Dirty appearance or discoloration is not a concern as long as the discoloration is uniform.

A5.2.2.4. Check to ensure the fiber pattern is not torn or disturbed.

A5.2.2.5. Check for any signs that glue has been applied to lifted or torn tape.

A5.2.3. If there is evidence of tampering, contact the SACCS-DTS library at DSN 271-4340 for instructions. Never use diskettes that have evidence of tampering.

A5.3. Tampering. If there is no evidence of tampering, destroy the blue logo tape by cutting the tape lengthwise. Dispose of the blue logo tape as unclassified waste.