

**BY ORDER OF THE COMMANDER
AIR FORCE GLOBAL STRIKE COMMAND**

**AIR FORCE GLOBAL STRIKE COMMAND
MANUAL 13-5201, VOLUME 5**



6 MAY 2026

Nuclear, Missile, Command and Control

**CODE CONTROL STANDARDIZATION:
PROCEDURES, TRAINING, AND
EVALUATION**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AFGSC/A3ON

Certified by: HQ AFGSC/A3O

Supersedes: AFGSCI 13-5201V5, 17 July 2020

Pages: 111

This instruction implements Air Force Policy Directive (AFPD) 13-5, *Air Force Nuclear Mission* and is consistent with AFI 13-520, *Aircraft and ICBM Nuclear Operations*; DAFI 91-101, *Air Force Nuclear Weapons Surety Program*; AFI 91-114, *Safety Rules for the Intercontinental Ballistic Missile System*; USSTRATCOM EAP-STRAT Volume 16, *ICBM Code Component Control Policy and Procedures*; and the Control and Management of National Security Agency Produced Information Security Materials for the ICBM Force. It establishes procedures and policies for the conduct of missile systems/codes flight (576 FLTS/DOX and OSB) activities and evaluation, training and certification of code handlers and code controllers. This instruction applies to Headquarters (HQ) Air Force Global Strike Command (AFGSC), Twentieth Air Force (20 AF), AFGSC missile wings, and the 377th Test and Evaluation Group (TEG). This instruction does not apply to Air Force Reserve, Air National Guard units, United States Space Force(USSF). This instruction requires collecting and maintaining information protected by the Privacy Act of 1974 authorized by 10 USC 8013. Privacy Act system notice number F036 AF PC C, Military Personnel Records System, applies. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) in accordance with [paragraph 1.3](#). Individual paragraphs to this instruction may only be supplemented by 20 AF. Supplements will not be less restrictive than the provisions of this publication and will be coordinated for AFGSC/A3O review prior to certification and publishing. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Product*. The authorities to waive wing, and unit level requirements in this publication are identified with a tier number (“T-0, or T-3”) following the compliance statement. See Department of the Air Force Manual (DAFMAN) 90-161, Publishing Processes and Procedures,

for a description of the authorities associated with the Tier numbers. Authority to waive compliance items is found in [paragraph 1.4.4](#). Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority in accordance with [paragraph 1.4](#). When a commander approves a waiver, the commander is communicating to superiors and subordinates that the commander accepts the risk by non-compliance. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) AFI 33-322, *Records Management and Information Governance Program*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). See [Attachment 1](#) for a glossary of references and supporting information.

SUMMARY OF CHANGES

This document has been substantially revised and must be completely reviewed. The document must be read in its entirety and in conjunction with the AFGSCI 13-5201V1-2, published Ready ICBM Program (RIP) Tasking Memorandum (RTM) and Ready Codes Program Tasking Memorandum (RCPTM) signed by AFGSC/A3. The changes are revised in response to a MAJCOM-level effort to standardize missile operations with Air Force operations.

Chapter 1—GENERAL INFORMATION	6
1.1. General.....	6
1.2. Clarification of Guidance (COG).....	6
1.3. Guidance Change Requests.....	7
1.4. Waivers.....	7
Chapter 2—ROLES AND RESPONSIBILITIES	9
2.1. Responsibilities.....	9
Chapter 3—CODE HANDLER FIELD OPERATIONS	12
3.1. Reporting.....	12
3.2. New START Inspections.....	12
3.3. Code Control Concepts.....	12
3.4. Team Composition.....	12
3.5. Code Categories.....	12
3.6. Complementary Code Components.....	13
3.7. Dispatch.....	13
3.8. LF Components.....	17
3.9. LCC Components.....	21
3.10. Holographic Tamper Detection Indicators (TDIs) (This section does not apply to the 377 TEG).....	25
3.11. Operation OLYMPIC STEP.....	28

Chapter 4—CODES VAULT OR SECURE AREA (OSB) OPERATIONS	31
4.1. Introduction.....	31
4.2. OSB Daily Operations.	31
4.3. ICBM Wing Coding Operations.	32
4.4. Missile Wing and 377 TEG Manning Requirements.....	33
Chapter 5—FACILITY AND SECURITY REQUIREMENTS	37
5.1. Physical Description.	37
5.2. Reports.	41
5.3. Deactivation Plans.	41
5.4. WCPS Coding Management Guide.	42
5.5. Locks.....	42
Chapter 6—CODING EQUIPMENT AND MATERIALS	43
6.1. General.....	43
6.2. Component Dispatch, Recovery and Team Briefings.....	43
6.3. Transfer and Shipping of COMSEC and Codes-Related Materials.....	44
6.4. Component Markings.	45
6.5. Inventories.	45
6.6. Failed or Broken Items.	46
6.7. Asset Tracking.	46
6.8. Documentation.....	46
6.9. LF Components.....	48
6.10. LCC Components (All TDI references do not apply to the 576 FLTS).....	52
6.11. OLYMPIC STEP.	55
6.12. Coding Operations.	55
6.13. WCPS Maintenance Requirements.....	61
6.14. Hardware Certification and Verification Equipment (HCVE).	61
Chapter 7—WEAPON SYSTEM TESTING	62
7.1. General.....	62
7.2. Simulated Electronic Launch Minuteman (SELM) (GIANT PACE) (This does not apply to the 377 TEG).	62
7.3. Hardness Surveillance Electromagnetic Pulse (EMP) Program (HSEP) (This does not apply to the 377 TEG).	63

Chapter 8—LATERAL CODING	66
8.1. General.....	66
Chapter 9—REPORTING	67
9.1. General.....	67
9.2. Possible Code Compromise (PCC).....	67
9.3. Possible Compromise of TDI Technology (PCTT).....	67
9.4. COMSEC Incident Report.....	67
9.5. DULL SWORD Reports.....	67
9.6. Termination of MCCM Rest.....	68
Table 9.1. Areas Affected During PCCs and PCTTs.....	68
Chapter 10—TRAINING AND EVALUATION REQUIREMENTS	69
10.1. Responsibilities.....	69
10.2. Codes Instructors.....	69
10.3. Training Materials.....	70
10.4. Code Handler Training (This does not apply to 377 TEG).....	71
10.5. Code Controller Training.....	73
10.6. Inactive Status.....	75
10.7. Code Controller Individual Qualification Folder (IQF).....	75
Chapter 11—CODE CONTROLLER EVALUATIONS	76
11.1. SCC/FC Responsibilities.....	76
11.2. ICBM Code Controller Standardization/Evaluation Officer Certification.....	76
11.3. Evaluations.....	77
11.4. Script Requirements.....	78
11.5. Evaluation Conduct.....	80
11.6. Post-Evaluation.....	81
11.7. Evaluation Debrief.....	83
11.8. Outbrief.....	83
11.9. Evaluation Ratings.....	83
11.10. Evaluation Documentation.....	84
11.11. Directed Training.....	85
11.12. Deficiency Reporting.....	85

Chapter 12—CERTIFICATION AND DECERTIFICATION	86
12.1. Code Handler and Code Controller Certification Program.....	86
12.2. Prerequisites for Certification of Code Controllers and Code Handlers.....	86
12.3. Code Handler Certification and Decertification (This does not apply to 377 TEG).	88
12.4. Code Controller Selection, Certification and Decertification.....	89
12.5. Code Controller Individual Qualification Folder.....	92
Chapter 13—MISCELLANEOUS	93
13.1. New or Upgrade System Requirements.....	93
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	94
Attachment 2—AFGSC FORM 165/166 REVIEW CHECKLIST	104
Attachment 3—CODE CONTROLLER INDIVIDUAL QUALIFICATIONS FOLDER REVIEW	105
Attachment 4—ICBM CODES SHIELDED ENCLOSURE REPAIR AND CERTIFICATION PROCESS	107
Attachment 5—CODES INVENTORY TABLE	109
Attachment 6—SHIELD ENCLOSURE PACE PLAN	111

Chapter 1

GENERAL INFORMATION

1.1. General. This instruction contains information necessary for the standardization of procedures, policies, evaluation, and training of coding operations for codes flights at intercontinental ballistic missile (ICBM) units and the flight test squadron. It provides requirements for certification of code handlers and code controllers. Additionally, this instruction captures operational requirements and standardized procedures to support the AFGSC mission.

1.2. Clarification of Guidance (COG). The intent of COG is to clarify guidance for operational units and ensure users possess a clear understanding of the policies outlined in this document. COG requests are not intended to address “what if” scenarios.

1.2.1. General. Submit COG requests on unit letterhead to AFGSC/A3ON through 20 AF/A3NB via e-mail: 20AF.A3NB.Workflow@us.af.mil. Requests must be routed through the group commander prior to submission. COG titles will consist of the subject and tracking number in the following format: two-digit year, two-digit month, three-digit unit. If multiple questions refer to the same subject matter, it is acceptable to combine them into a single request. If the questions are not on the same subject matter, submit them separately. For COG related to weapon system operations or United States Strategic Command (USSTRATCOM) procedures, 20 AF/A3NB will coordinate with AFGSC, USSTRATCOM, and other agencies as needed. All COG will be coordinated with AFGSC/A3ON for final determination regarding instructions and regulations prior to issue.

1.2.2. COG Management. 20 AF/A3NB is the AFGSC/A3ON delegated OPR to receive, research, coordinate, and prepare official COG memoranda. Additionally, 20 AF/A3NB is responsible for distribution of formalized COG IAW [paragraph 1.2.5](#) of this regulation and maintaining a repository of all current COG memoranda.

1.2.3. COG Conference. 20 AF/A3NB will ensure COG is properly coordinated with concerned agencies to address topics of concern, assess sense of urgency, and recommend initial position for the formal reply.

1.2.4. HHQ Suspense for Reply to Units. Within 15 working days, the MAJCOM / 20 AF will provide a complete answer or notify the unit that further coordination with other units is required and provide a projected timeline.

1.2.5. COG Distribution. All formal COG responses will be distributed to the following agencies, as a minimum: 90 OSS/OSB, 91 OSS/OSB, 341 OSS/OSB, 377 TEG, AFGSC/A3ON, USSTRATCOM/J374, and NSA/C62. Distribute to HAF AFSEC/SEW, AFNWC/NI, AFGSC/SEW, AFGSC/IG, NGAS, and Boeing Layton, as needed.

1.2.6. Final Authority for ICBM Codes System and Procedures COG. 20 AF/A3NB is the final authority for all COG regarding procedural and technical order questions. 20 AF/A3NB will evaluate and respond to COG for procedural and technical order questions. 20 AF/A3NB will engage AFGSC/A3ON for compliance with this publication. Other agencies will be included in coordination as needed.

1.2.7. Final Authority for ICBM Codes Standardization, Evaluation, and Training COG. As OPR for this instruction, AFGSC/A3ON is the final authority for all COG regarding Evaluation, Training, and Certification.

1.2.8. Inspector General. AFGSC/IG identified findings that involve ICBM codes COG will be coordinated with AFGSC/A3ON, who will, as necessary, coordinate with 20 AF/A3NB prior to validating the finding.

1.3. Guidance Change Requests. Submit recommended changes for this publication to the OPR, AFGSC/A3ON, 245 Davis Avenue East, Barksdale AFB, LA 71110 or to the A3ON workflow email AFGSC.A3ON.Workflow.1@us.af.mil using the DAF Form 847 and the *HQ AFGSC AF Forms 847 and Flight Manuals SharePoint Site*.

1.3.1. Coordinate and route DAF Form 847s through the chain of command.

1.3.2. Changes submitted for approval must include concurrence or non-concurrence recommendations/comments from all affected OGs prior to transmission. In the event a unit does not receive a response from an affected OG in a reasonable amount of time, the submitted changes should include a statement identifying that no response was received.

1.3.2.1. Initiating unit will send the DAF Form 847 to 20AF.A3NB.Workflow@us.af.mil. 20 AF will provide coordination with other OGs and other staff agencies, as required. The request will then be moved to the “MAJCOM COORD” tab. Provide notification verbally or via email of upload.

1.3.2.2. The publication OPR will maintain all approved DAF Form 847s and is responsible to ensure all changes are incorporated into the next available interim change or publication rewrite.

1.4. Waivers. AFGSC/A3 is the waiver authority for this instruction unless specifically stated otherwise. Waiver authority may not be delegated. Waivers will be granted on an individual basis.

1.4.1. Forward all waivers via e-mail through 20 AF/A3NB to AFGSC/A3ON describing the specific requirement creating the problem and explaining why a waiver is needed. Waivers will be drafted using AF Form 679. 20 AF will add recommendation(s) within the requested waiver, and then forward to AFGSC/A3ON, who will add recommendation(s) and forward to AFGSC/A3 for a final determination.

1.4.2. Waivers must include quoted instruction requirement references along with adequate background information, justification, and mission impact if waiver is not granted.

1.4.3. If approved, waivers remain in effect for 30 days following the approving commander's change of command, unless the new commander renews the waiver or AFGSC/A3 states a specific period of time, cancels the waiver in writing, or issues a change that alters the basis for the waiver. Rationale will be provided within the waiver response.

1.4.4. The authorities to waive wing/unit level requirements in this publication are identified with a Tier (“T-0, T-3”) number following the compliance statement. See DAFMAN 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the Publication OPR for non-tiered compliance items. When the waiver authority approves a commander's waiver request, the waiver authority and the submitting commander are communicating to superiors and

subordinates that they are accepting the risk of non-compliance. Per DAFI 90-160, “commanders/directors may waive non-tiered compliance items, but must send a copy of the approved waiver to the OPR of the higher headquarters publication being waived within 30 days of approval. (T-1)”

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. Responsibilities. The control of ICBM codes and code components is primarily the responsibility of all certified code handlers and code controllers. This responsibility is not, however, limited to these individuals. Commanders and supervisors of code handlers, code controllers, and all other individuals whose duties involve or affect the control of codes share the responsibility for compliance with the requirements of this instruction.

2.1.1. The Commander, USSTRATCOM is the Controlling Authority (CONAUTH) for all ICBM keys and codes and material supporting ICBM weapon system operations. USSTRATCOM/J374 is responsible to the CONAUTH, to manage all ICBM keys, codes, and supporting materials. Reference EAP-STRAT Volume 16 for additional applicable responsibilities.

2.1.2. AFGSC/A3ON. Provides policy guidance, in conjunction with 20 AF/A3NB, to support USSTRATCOM and HHQ, for ICBM launch control and code system security and safety. In addition, AFGSC/A3ON, in conjunction with 20 AF/A3NB, plans, coordinates, directs, and monitors Operation OLYMPIC STEP actions. AFGSC/A3ON will serve as the AFGSC representative for staff assistance visits, standardization, evaluation and in matters concerning the design, development, implementation, and maintenance of ICBM launch control and code systems, system software, and code components, provide guidance on manning, training, and evaluation requirements for ICBM code handlers and code controllers, serve as the HQ representative to non-Air Force agencies and other organizations in matters pertaining to ICBM launch control and code system security and safety, publish and maintain AFGSCMAN 13-5201V5, provides funding and support for ICBM launch control, code systems, holographic Tamper Detection Indicators (TDIs) and USSTRATCOM/J374 Strategic Air Command (SAC) Code Processing System (SCPS) equipment.

2.1.3. 20 AF/A3NB. Responsible for providing technical expertise and serves as an operations liaison between AFGSC/A3ON, USSTRATCOM/J374, and units for code related operations policy clarifications, enforcement of standardization and evaluation standards, management of technical orders, and coordinates code control group change requests and forwards to AFGSC/A3ON and USSTRATCOM/J374 for approval. Facilitates the standardization of unit coding operation plans, training, and evaluation programs. Managerial responsibilities include serving as HQ AFGSC technical experts for design, development, and implementation of ICBM launch control and code systems, system software, and code components. May be utilized to augment HQ AFGSC staff regarding inspections and SAVs, as requested.

2.1.4. 377th Test and Evaluation Group/576 FLTS/DOX. Responsible for the proper configuration of ICBM codes systems, critical components, and miscellaneous devices supporting Force Development Evaluation (FDE). Provides test and evaluation support to AFGSC, Air Force Materiel Command (AFMC), Air Force Nuclear Weapons Center (AFNWC), Air Force Operational Test and Evaluation Center (AFOTEC), USSTRATCOM, and Department of War (DoW) contractors for special tests and studies, lateral coding, contractor kit and Technical Order (T.O.) proofing, and Wing Code Processing System (WCPS) code controller training as directed by HQ AFGSC. Will control test ICBM codes and critical components according to EAP-STRAT Vol 16. Responsible for managing the ICBM

secure code system for their respective unit mission. This responsibility includes training of unit code controllers. All unit code controllers must be certified per EAP-STRAT Vol 16 and this publication. Will provide staff and technical assistance to the commander on all matters pertaining to ICBM code operations through the preparation and maintenance of plans tailored for their respective unit's mission. Responsible for reporting incidents involving critical components, code components, and other COMSEC account material under their control to USSTRATCOM/J374, AFGSC/A3ON, 20 AF/A3NB, and providing an information copy to DIRNSA/C62. The 377 TEG does not have code handlers and any references to requirements concerning code handlers are not applicable.

2.1.5. Unit Codes Flight (OSB). Responsible for managing the ICBM secure code system for their respective wing mission. This responsibility includes oversight and support of code handler and code controller training programs, training of code controllers and code handlers, and management of wing codes familiarization program. All code handlers and code controllers must be certified per this instruction and the EAP-STRAT Vol 16. Will provide staff and technical assistance to the commander on all matters pertaining to ICBM code operations through the preparation and maintenance of plans tailored for their respective wing's mission. Responsible for creating and maintaining a lateral coding relocation and support plan. Responsible for reporting incidents and possible incidents involving critical components, code components, and other COMSEC account material under their control to USSTRATCOM/J374, AFGSC/A3ON, 20 AF/A3NB, and DIRNSA/C62.

2.1.6. National Security Agency (NSA). Reference EAP-STRAT Vol 16 for applicable responsibilities.

2.1.7. 532nd Training Squadron (532 TRS). Will provide basic code handler training during Initial Skills Training (IST). This training does not fulfill requirements for Initial Codes Training (ICT) at the gaining operational unit.

2.1.8. AFGSC Weapons Safety Division (AFGSC/SEW). Responsible for AFGSC Nuclear Surety Policy directives and operational certification/decertification of nuclear related systems within AFGSC. Serves as the AFGSC voting member and point of contact for all Nuclear Weapon System Safety Group (NWSSG) studies and actions on AFGSC weapon systems (e.g., Operational Safety Reviews and Special Safety Studies, Weapon System Safety Rules (WSSR)). Reviews all DULL SWORD reports for trends and cross-tell analysis.

2.1.9. Air Force Nuclear Weapons Center Minuteman III Systems Directorate (AFNWC/NI). Designated program manager for design and development of the ICBM Code Processing System (ICPS) and all hardware and software Common Certification Operating System (CCOS), WCPS Minuteman (MM) Application Program (WMAP), SCPS Application Program (SAP) and Hardware Certification Verification Equipment (HCVE) (online and offline diagnostics) and modifications to them. AFNWC/NI is the depot for, and provides the item manager and equipment specialist for, the Code Change Verifier (CCV), Data Transfer Unit (DTU), Mechanical Code Unit (MCU), Launch Control Panel (LCP), Launch Enable Panel (LEP), and Command Signal Decoder (Missile) (CSD(M)). AFNWC/NWI, Safety, Environment and Engineering Data Branch (AFNWC/NWIEV) is the TO Management Authority (TOMA) for T.O.s 31X8-2-2-1, *Operation Instructions, Console, Wing Code Processing System (WCPS) (P/N 10365-107-())*; 31X8-2-2-2, *Maintenance Instructions with Illustrated Parts Breakdown, Console, Wing Code Processing System (WCPS) (P/N 10365-*

107-()); 31X8-2-3-1, Operation and Maintenance Instructions with Illustrated Parts Breakdown, Console, Hardware Certification Verification Equipment (HCVE) (P/N 11800-315-11); and 21M-LGM30F-12-1, Minuteman Nuclear Surety Procedures for the WS-133A-M Weapon Systems.

Chapter 3

CODE HANDLER FIELD OPERATIONS

3.1. Reporting. Any violation of this instruction or improper handling of the components and materials listed herein must be reported to the Wing OSB/576 FLTS DOX codes vault or secure area immediately, providing the information required by EAP-STRAT Vol 16. Based on the conditions and material involved additional reports may be required (e.g., DULL SWORD, COMSEC). **(T-0)**

3.2. New START Inspections. Suspend all coding activities for training or emergency, routine or annual while treaty inspectors are present on base or in the missile complex. Do not dispatch any code or code related materials anywhere in the ICBM missile or test complex. Coding activities may resume upon the treaty inspectors' physical departure from base and complex. **(T-0)**

3.3. Code Control Concepts. For specifics on code control requirements, to include component control and control group designation, reference the EAP-STRAT Vol 16.

3.3.1. Installation. Proper installation of a code component is defined as a code component being installed according to this publication and appropriate technical orders. **(T-0)**

3.3.1.1. Launch Control Center (LCC) Installation. One awake MCCM and holographic TDIs are used to provide Two Person Control (TPC) control in the LCC while the other MCCM is in rest status and the LCC blast door is closed. The exception is when the translate code values have been inserted into the WSP; crew rest is not authorized in order to control the translate code values. **(T-0)**

3.3.1.1.1. **[576 FLTS Only].** When Task Force MCCM are present, only one MCCM is in the LCC while the other is in crew rest status. The exception is when the visitors/maintenance are present in the LCC. 576 FLTS personnel will follow local procedures when components are in the LCC.

3.3.1.2. Launch Facility (LF) Installation. When all code components are properly installed in a LF the minimum control required is a TPC team. **(T-0)**

3.3.1.2.1. **[576 FLTS Only].** No special control.

3.4. Team Composition. Code system and component design features offer a high degree of security and safety, but the ultimate protection for system operations is provided by code handling teams. These teams are DoW personnel who must be trained, qualified and certified as code handlers. They are fully qualified to fulfill TPC requirements and are the only individuals entrusted with the control of operational code components. **(T-0)**

3.4.1. Code Handlers and Code Handling Teams. Officer and enlisted personnel are appointed as code handlers; a minimum of two code handlers are used to form a code handling team. All code handlers are assigned to code control Group X. **(T-0)**

3.4.2. Field Coding Operations. For field coding operations a team composed of any two code handlers (XX) is used to control those code components which do not require two officer control.

3.5. Code Categories. There are two categories of ICBM codes: operational and test.

3.5.1. Operational Codes. An operational code is one in operational use or planned for operational use in Emergency War Order (EWO)-configured (coded with proper codes and targeting information to execute launch command) LFs or LCCs.

3.5.2. Test Codes. Test codes are identical in format to operational codes but are designated and used only for test and training purposes. The controls outlined for operational code components do not apply to test code components; however, to meet training, exercise, evaluation, or test objectives, operational controls will be applied to test materials. Test and training Launch Facility Load Compact Disks (LFLCDs) produced by an operational WCPS are critical components and require TPC. LCPs, LEPs, and CCVs will retain their operational control regardless of whether they contain test or operational codes.

3.6. Complementary Code Components. Certain combinations of code components could provide knowledge of the entire code used to enable or launch a missile or allow unrestricted access to code components. Therefore, enable and launch codes are split to protect the Worldwide Unlock and Launch Codes. Complementary code components are listed in the EAP-STRAT Vol 16. Field components are not complementary, but teams will still require knowledge of the tasks to be performed in order to spot unauthorized acts and therefore teams should remain in control of the components they are trained to operate (i.e., no mixed teams of Missile Maintenance Team (MMT) and Electro-Mechanical Team (EMT)).

3.7. Dispatch. Any team used for tasks affecting the proper installation of code components or require the handling, receipt, control, or transfer of code components, critical components, programs, or OSB-issued miscellaneous materials will receive a briefing from OSB/576 FLTS DOX code controllers on their code handling responsibilities before they leave the Missile Support Base (MSB) or arrive at the FDE site. Any team accomplishing code handler duties involving code, critical, or miscellaneous components/items will receive a briefing from OSB prior to any follow-on travel at the discretion of OSB. OSB code controllers will verify all team members are certified under the Personnel Reliability Program (PRP) and meet code handler training requirements prior to allowing the team to handle code materials. 576 FLTS/DOX code controllers will develop and maintain their own method for verifying dispatch teams as they do not have code handlers. Reference EAP-STRAT Vol 16 for components, programs, and materials applicable.
(T-0)

3.7.1. Transportation of Code Components to and from the LF/LCC/Missile Alert Facilities (MAF). Rules for transportation of code components between the MSB, LFs, LCCs and MAFs are listed below:

3.7.2. First Stop/Last Stop Rule. Except for Reentry System/Reentry Vehicle/Propulsion System Rocket Engine (RS/RV/PSRE) convoys, OSB will be the last stop enroute to the coding location and the first stop upon returning to the MSB. Exceptions are granted by OSB on a case-by-case basis. This does not apply to the 377 TEG.

3.7.3. Unauthorized/Unscheduled Stops. When transporting code components outside OSB the code handling team is prohibited from making any unauthorized or unscheduled stops. If the code handling team must make an unauthorized stop, Missile Maintenance Operations Center (MMOC) and OSB will be notified immediately, OSB will then notify USSTRATCOM/J374 and report the Procedural Violation (PV) as defined in the EAP-STRAT Vol 16. Only OSB can authorize a deviation from the approved code handler itinerary. This does not apply to the 377 TEG.

3.7.4. **Unscheduled Maintenance.** MMOC must notify OSB before diverting a code handler team to a MAF or LF not on the approved code handler itinerary. Every effort must be made to return codes to the OSB as expeditiously as possible. For example, if a team will pass by the MSB when diverting from one site to another, the team will stop at OSB to secure code material before proceeding. This does not apply to the 377 TEG.

3.7.5. **Code Component Control, TPC, and Security.** During transport, control and security for code components will always be provided by the appropriate code handling team, using visual observation as described in this publication.

3.7.6. **Vehicles.** Code components will only be transported in a military vehicle. **(T-0)**

3.7.6.1. Code handlers will transport code components in an enclosed vehicle. Open bed trucks do not offer protection from theft, loss, environment, etc. **(T-0)**

3.7.6.2. The enclosure must be lockable. **(T-0)**

3.7.6.2.1. **[377 TEG Only].** Enclosed vehicles or vehicles without an enclosure containing test or training components do not require locks, except to satisfy operational realism requirements.

3.7.6.3. Code handlers must be able to maintain visual observation of code components while components are in the enclosure. **(T-0)**

3.7.6.4. A damaged enclosure permitting access by an individual or exposure to the environment (inoperative lock(s), glass pane broken, etc.) will not be used. **(T-0)**

3.7.6.5. **Radios.** When transporting code components outside of the Mission Support Base (MSB), the military vehicles (air or ground) or the military convoy they are traveling in must be equipped with an operational radio and accomplish radio security checks every 15 minutes with an on-base agency (i.e., Missile Field Control Center (MFCC), Missile Security Control (MSC)). Team will relay through a Flight Security Controller (FSC) if unable to directly contact the on-base agency. This does not apply to the 377 TEG.

3.7.7. **LCP Transportation Restrictions.** Coded LCPs must be separated by 30 minutes travel time from other LCPs for the same squadron. This restriction does not apply during Emergency Combat Capability (ECC) preparation, when returning superseded and test codes, or to the 377 TEG. **(T-0)**

3.7.8. **Locks.** Code component cases containing codes and/or electronic keys will be locked with two locks when transported outside the confines of the MAF, LF, or MSB. MCCMs may use their crew locks (or locks provided by OSB) to transport codes to and from the LCC. Additionally, courier teams may utilize MCCM style crew locks to transport components from the MSB to an authorized code handler team provided the team has the appropriate locks as described in this publication when they receive the component from the courier team. This does not apply to the 377 TEG. **(T-0)**

3.7.9. **Field Storage.** Field storage procedures for code components will be used whenever a code handling team cannot maintain visual observation and the code components are not properly installed.

3.7.9.1. **Code Handler Responsibilities for Field Storage.** Any time field storage of code components is required, code handling teams will notify OSB/576 FLTS DOX (and follow

their instructions), the Missile Maintenance Operations Center (MMOC), and the Missile Combat Crew (MCC) in control of the flight area where the code components will be placed into field storage.

3.7.9.2. Removal from Field Storage. The code handling team will notify OSB/576/DOX, MMOC, and the MCC in control of the flight area when code components are removed from field storage.

3.7.9.3. The 576 FLTS/DOX will ensure teams comply with DoDM5200.01V3_DAFMAN16-1404V3, Information Security Program: Protection of Classified Information, AFI 16-1404, COMSEC regulations, and local security regulations when storing classified material in unmanned test LCCs or LFs.

3.7.9.4. MCC Responsibilities. When code components are stored in the LCC or at an LF, the MCC with primary responsibility will (these do not apply to the 377 TEG):

3.7.9.4.1. Log field storage/removal notification in the crew log and brief it at every MCC changeover while the item is field stored. Additionally, the MCC will log removal from field storage when notified by the code handling team.

3.7.9.4.2. Ensure access to the stored component(s) is limited to the proper team. **(T-0)**

3.7.9.4.3. If codes are in field storage topside at an LF, the MCC must brief each team entering the LF that codes are in storage.

3.7.9.4.4. If codes are stored in the Launcher Equipment Room (LER) each team authorized LF penetration will be briefed that codes are in field storage.

3.7.9.4.5. Code components stored in the LCC must be awaiting installation or removal from that LCC and must be sealed with holographic TDIs in approved storage cases before the MCC can go into rest status. Uninstalled holographic TDIs may be stored in the same case with these components. See the EAP-STRAT Vol 16 for TDI installation requirements. **(T-0)**

3.7.9.4.6. Remote Data Change-Codes (RDCC) and Remote Data Change-Keys (RDCK) Removable Storage Media (RSM) may be stored in the LCC. They must be inventoried by the on-coming MCCMs and properly labeled in order to maintain accountability.

3.7.9.5. Special Field Storage Instructions. These do not apply to the 377 TEG.

3.7.9.5.1. Guards. A TPC team must guard code components in field storage topside at the LF or MAF. **(T-0)**

3.7.9.5.2. CCV Field Storage. The approved CCV tamper-evident bag (supplied with the CCV) must be used any time the CCV is placed into field storage. **(T-0)**

3.7.9.5.3. Locks. Components must be locked with two code handler locks (locks are not required for field storage of code components in the LCC). These locks will be secured on the carrying case, tamper-evident bag, or the vehicle, as appropriate. Refer to [paragraph 5.5](#) of this publication for lock requirements. **(T-0)**

3.7.9.5.4. Missile Guidance Set (MGS) Vault. Vault must be locked with two locks and must meet the criteria of a vault as defined in DoDM5200.01V1_DAFMAN16-

1404V1, Information Security Program: Overview, Classification and Declassification, and DoDM5200.01V3_DAFMAN16-1404V3. The vault must be alarmed or guarded by a TPC team if the alarm is inoperative. This TPC team must be furnished with a list of code handlers authorized entry to the MGS vault. **(T-0)**

3.7.9.5.5. LER. The LF must satisfy all current security requirements or have appropriate guards posted per DoDM S-5210.41-MV3_AFMAN 31-108V3_AFGSCSUP, Enclosure 6 and **AFI 91-114**. Locked containers must be secured to a permanent structure to meet hardness requirements. **(T-0)**

3.7.9.5.6. PT Van. Secure both the launch tube access door (cam locks are locked) and the emergency egress door from inside the van. The personnel access and rear doors must each be locked with two code handler locks (this does not apply to the 377 TEG). **(T-0)**

3.7.10. Field Transfer. Field transfer of code or critical components and miscellaneous materials will occur inside the fenced areas of the LF or MAF; exceptions must be pre-coordinated and approved by OSB/576 FLTS/DOX.

3.7.10.1. Code Handler Responsibilities. If a code handling team must transfer code or critical components or miscellaneous materials to another code handling team in the field, the team chief will notify OSB prior to field transfer. Maintenance teams should complete AF Form 1297 Hand Receipt or other locally produced hand receipt to transfer code or critical components and return the completed form(s) to OSB/576 FLTS upon arrival at support base.

3.7.10.2. OSB/576 FLTS/DOX Responsibilities. When notified of a field transfer requirement OSB will:

3.7.10.2.1. Verify the code handling status of the team receiving the components. **(T-0)**

3.7.10.2.2. Provide a code handler briefing to the code handling team assuming control of the code components. This briefing may be accomplished by telephone or radio. **(T-0)**

3.7.10.2.3. Notify the MCC in control of flight area to inform them of the field transfer. This applies to the 576 FLTS when a crew is on duty. **(T-0)**

3.7.11. LF Penetration. The minimum controls required for LF penetration are listed below. These do not apply to the 377 TEG.

3.7.11.1. Properly Installed Components. If all code components are properly installed in the LF the minimum team required to penetrate the LF is a TPC team. **(T-0)**

3.7.11.2. Proper Field Storage. If an LF contains a properly field stored code component, the minimum team required to penetrate the LF is a TPC team. **(T-0)**

3.7.11.3. Components Not Properly Installed or Stored. MMOC and OSB will be notified whenever a code component is not properly installed or stored in the LF. If an LF contains code components not properly installed or field stored, a code handler team (XX) must be the last to depart and first to penetrate the LF and enter the LER. The only exception to this rule involves the CSD(M). See EAP-STRAT Vol 16 for details. **(T-0)**

3.7.12. Evacuation and Re-entry. These do not apply to the 377 TEG.

3.7.12.1. LER Evacuation. If a situation necessitates evacuation of the LF LER, the maintenance team chief will ensure access to the LF LER is controlled by a TPC team IAW technical data. If components are not properly installed, control LER access with a code handler team (XX). The team controlling entry to the evacuated LF LER will not guard any other code or critical component(s) at the LF. **(T-0)**

3.7.12.2. LER Re-entry. Re-entry requirements for an evacuated LER are the same as penetration requirement described in LF penetration paragraphs above. A Possible Code Compromise (PCC) will be declared if conditions in paragraphs 3.7.11 through 3.7.11.3 are not met during LF reentry. **(T-0)**

3.7.12.3. LCC Evacuation. If the MCC departs the LCC for any reason, and code component(s) are properly installed, or field stored a TPC team will control entry to the LCC. One member of the team must be an MCCM. The team controlling entry to the evacuated LCC will not be used to guard any other code or critical component(s). When the LCC is evacuated, the “No Lone Zone” is extended to the security control center door. If the exterior access door or the door to the elevator shaft is open, two MCCMs will guard entry to the LCC by posting in the elevator shaft-way. An LCC de-postured to TPC control (all components removed or administratively decertified IAW the T.O. 21M-LGM30F-12-1, and the EAP-STRAT Vol 16) does not require an MCCM as part of the guarding team. **(T-0)**

3.7.12.4. LCC Re-entry. The first team to re-enter an LCC with operational codes will be a two-officer code handling team (MCC). A PCC will be declared if the first team to reenter the LCC is not the proper code handling team for the installed components. **(T-0)**

3.7.13. Computer Memory Security Check (CMSC). CMSCs are computed to ensure the proper load of the LFLCD data via DTU. This number will be compared with the OSB/576 FLTS CMSC computed by the WCPS. If OSB/576 FLTS is closed, the CMSC may be compared with the CMSC provided by OSB/576 FLTS to the unit command post. A combination of two personnel (OSB code controllers or Command Post controllers) will compare the CMSC computed by the maintenance team with the WCPS-computed CMSC. Missiles will not be placed on alert until these CMSCs match. **(T-0)**

3.7.13.1. **[377 TEG Only]**. One MMOC controller or 576 FLTS code controller may compare the value obtained at the LF with the WCPS-computed CMSC. **(T-0)**

3.7.13.2. Invalid CMSC. A CMSC is invalid if, after initiating DTU load, no CMSC, an incomplete CMSC, or any CMSC other than the one computed on the WCPS is obtained. When an invalid CMSC occurs, the code handling team must call the MCC, MMOC, and OSB/576 FLTS for maintenance team back out procedures and LF closure instructions (IAW T.O. procedures).

3.8. LF Components. Operations involving LF code, critical and miscellaneous components for the Minuteman weapon system are outlined below. For control of code components, reference the EAP-STRAT Vol 16. Transport and storage limitations listed here do not apply to the 377 TEG. Proper installation of components listed below do not reference any requirements directed by applicable technical orders.

3.8.1. P-Plug. P-Plug contains the LF unique portion of the launch code. It is classified Top Secret. Test P-Plugs for FDE are Unclassified. **(T-0)**

3.8.1.1. Proper Installation. P-Plugs will only be installed or removed at the LF. The P-Plug is properly installed when it is in the MGS, the MGS is on the missile in the launcher and the RS is mated on the MGS. **(T-0)**

3.8.1.2. Transport. Transport all uninstalled P-Plugs in a locked case. Do not transport P-Plugs while installed in an MGS. **(T-0)**

3.8.2. Complete Load LFLCD. The complete load LFLCD will be loaded onto the DTU which will contain PEN DATA, I Codes, Operational Ground Program/Operational Flight Program (OGP/OFP), flight constants, and MGS Parameters Data. It is classified Secret.

3.8.3. Proper Installation. The LFLCD data has been properly installed when it has been locked in the MGS computer with a PEN C Code and the CMSC computed by the maintenance team has been verified by either two controllers from OSB/576 FLTS or the unit command post with the WCPS-computed CMSC. **(T-0)**

3.8.3.1. **[377 TEG Only]**. One MMOC controller or 576 FLTS code controller may compare the value obtained at the LF with the WCPS-computed CMSC.

3.8.4. PEN D LFLCD. A DTU containing PEN D LFLCD data contains PEN data to unlock the Missile Guidance Computer (MGC) for local overwrite. It is classified Secret. The DTU containing PEN D LFLCD data contains only PEN data. **(T-0)**

3.8.5. MGC. The MGC, located in the MGS of each missile provides missile programming, targeting, status monitoring capability, storage of launch critical codes and execution data.

3.8.5.1. Overwritten or New MGS Computer. An operational, overwritten, or new MGS computer is a critical component. An overwritten or new MGS computer is classified Secret. The 377 TEG does not OPCERT the Test MGS. **(T-0)**

3.8.5.2. MGS Computer Failed Overwrite. A coded MGS that fails remote or local overwrite may be manually cleared of coded memory by MMT prior to demate by disconnecting the Static Random Access Memory (SRAM) battery per appropriate technical data. A code handler team must be present during SRAM battery disconnect procedure. The SRAM battery disconnect procedure erases fault and history data Boeing Guidance Repair Center (BGRC) requires to properly repair the MGC within the MGS. Therefore, SRAM disconnect will only be used as a last resort except in cases when technical data specifically prohibits the use of remote and/or local overwrite. Once the memory is cleared in this manner and 15 minutes have elapsed, MGS control is TPC. A coded MGC that fails the overwrite terminate portion of the overwrite sequence is considered to have failed overwrite and will be controlled by a proper code handling team (XX) IAW EAP-STRAT Vol 16. **(T-0)**

3.8.5.3. PEN C-coded MGS Computers. A PEN C-coded MGS computer is the result when the computer has been remotely overwritten, but with no overwrite terminate command issued by the LCC or improper terminate indications. The MGS computer contains only PEN C data. The MGS computer can be sent through normal channels to the BGRC after codes supersession. **(T-0)**

3.8.5.4. Proper Installation. An MGS computer is properly installed when it is locked with a PEN C Code, a CMSC has been computed and verified and the MGS is on the missile in the launcher. **(T-0)**.

3.8.6. MGS Computer Overwrite. An MGS computer will be overwritten before it is removed from the LF fenced area when possible. This rule does not apply to test-coded training LF MGSs removed to support Force Generation. Control an operationally coded MGS computer which fails to overwrite IAW this publication. If remote or local overwrite attempts fail, disconnecting the SRAM battery for 15 minutes can manually clear the operational code data in an MGC failing overwrite (IAW T.O. procedures). **(T-0)**

3.8.6.1. Remote LF Overwrite. The MCC performs remote LF overwrite when directed by MMOC and in conjunction with OSB/576 FLTS. The MCC will notify MMOC and OSB/576 FLTS with overwrite results. If the remote attempt fails, local overwrite may be attempted. If the remote attempt fails at overwrite terminate, the MGS is considered in an unknown state and should be treated as if codes remain. The MCC will notify OSB/576 FLTS/DOX, MMOC, all maintenance teams who penetrate the LF and their relief MCC of the MGS computer overwrite status until the MGS has been replaced or recoded. The MCC documents a successful overwrite and returns the completed overwrite documentation to OSB/576 FLTS. **(T-0)**

3.8.6.2. The local overwrite procedure of an MGS will be accomplished by a code handling team (XX). Using the DTU to initiate the overwrite program stored in the MGC within the MGS. The code handling team accomplishing the local overwrite will notify OSB/576 FLTS, the MCC, and MMOC of the local overwrite procedures results. The 576 FLTS does not need to use code handlers for this procedure. **(T-0)**

3.8.7. Code Change Verifier (CCV). The CCV is used to encode the CSD(M) with operational/test enable codes or a maintenance code. Before dispatching with a CCV, code handling teams will verify what code (operational, test, or maintenance) will be loaded into the CSD(M) with the MMOC and OSB/576 FLTS. **(T-0)**

3.8.7.1. Field Operations. When a CCV is used to perform CSD(M) Code Change Procedure, the LF launcher closure door must be shut, no land line communications may be used, and only personnel directly involved in the coding operation IAW T.O. 21M-LGM30G-2-12-2, Computer Program Loading and Command and Status System Maintenance or required to maintain proper control of a code component will be allowed in the launcher. Use of the Personnel Alarm System (PAS) is authorized. **(T-0)**

3.8.7.1.1. CCV Verification Number (VN). Coding a CSD(M) with the CCV results in a unique VN. This number will be displayed after coding a CSD(M) and it must match the VN computed by the WCPS before the missile can be called on alert. At least one OSB/576 FLTS code controller, command post, or MMOC controller will verify the VN. When a VN mismatch occurs, maintenance code handlers will follow instructions provided by MMOC and OSB/576 FLTS. **(T-0)**

3.8.7.2. OSB Operations. All CCVs used to insert or remove a code must be verified using the WMAP Trace/Verify CCV procedure as soon as possible after recovery. If the verification of a CCV used to insert an operational code fails or the trace data does not indicate a successful CCV run, remove, and withhold the missile from alert and apply

operational controls until a successful trace/verification is achieved. If the trace/verification of a CCV used to remove an operational code fails, apply operational controls to the affected missile(s) until a successful CCV trace/verification is achieved. CCV trace/verification data will be printed immediately after unloading the data onto the WCPS data disk. **(T-0)**

3.8.8. CSD(M). The CSD(M) is an electro-mechanical stepping decoder located on top of the MM first stage. The CSD(M) provides continuity for the missile ignition safe/arm device for the first stage. **(T-0)**

3.8.8.1. Proper Installation. An operational CSD(M) is properly installed when the missile is in place (on the support ring) in the LF and the CCV VN matches the VN computed by the WCPS. In the event of a problem obtaining a correct VN, if OSB/576 FLTS/DOX can determine the coding of the CSD(M) via weapons system indications (such as trace data, wrong site ID procedures, etc.), then an operational CSD(M) can be considered properly installed. **(T-0)**

3.8.8.1.1. Improper Installation. Improper installation will result from an incorrect or no VN after attempting to load the CSD(M) with a CCV. An exception is granted to the site penetration rules in this case due to the CSD(M)'s location in the missile which prevents physical access or removal while in the field. **(T-0)**

3.8.8.2. Field Operations. Prior to dispatching a missile downstage from MSB, a maintenance code will be loaded into the CSD(M) to verify proper operation. Do not place an operational RS/RV on a missile until an operational code is installed and verified (good VN) in the CSD(M) IAW **AFI 91-114**. Additionally, do not remove an operational code from a CSD(M) until the RS/RV has been removed. **(T-0)**

3.8.8.3. Decertify a CSD(M) when the operational L' Code is replaced with a non-operational code (maintenance). ICBM units will administratively supersede the operational L' code previously inserted in the fielded CSD(M) when all T.O. directed actions to insert the maintenance code have failed. If the CSD(M) cannot be coded with a maintenance code, establish the appropriate control with the start of missile removal from the missile support ring. A code handler team (XX) will observe the removal of the CSD(M) at the MSB and will return the coded CSD(M) to OSB. OSB will store the CSD(M) in a split-handled container of the appropriate control group in the vault or Shielded Enclosure (SE) until supersession of the operational code. When the CSD(M) is returned to depot for repair, it is decertified and declassified when the TPC team and repair facility technicians verify the code has been erased. Code handler controls are not required for 576 FLTS. **(T-0)**

3.8.9. TSEC/KS-60. The KS-60 contains the active and reserve keys necessary for all encryption or decryption of message traffic between the LCC (Hardened Intersite Cable System (HICS) key) and LF (HICS key). Additionally, there are specific keys loaded from the WCPS to the TSEC/KS-60 within the SE and are taken from a pool of keys previously loaded to the WCPS from the Wing Pool Key CDs. The keys are designated as Traffic Encryption Key (TEK), Key Encryption Key (KEK), Recode Encryption Key (REK) upon loading on the WCPS. The Irreversible Transformation Key (ITK) is loaded to the WCPS via the ITK CD from USSTRATCOM/J374. Only nuclear-certified KS-60s listed on COMSEC account 613202 shall be used in operational LFs, LCCs, and WCPSs. **(T-0)**

3.8.9.1. Control. A keyed KS-60 is classified at the highest level of the keys, normally Top Secret//CRYPTO//NOFORN in operational use. An un-keyed KS-60 is classified Secret//CRYPTO//NOFORN. OSB may direct battery removal of a keyed KS-60 for the specific purpose of dissipating electronic keys and the KS-60 reverts to Secret//CRYPTO//NOFORN. KS-60s used at the 576 FLTS are not critical components and are controlled by classification only. Reference EAP-STRAT Vol 16 for proper control/handling requirements. **(T-0)**

3.8.9.2. Proper Installation. The KS-60 is properly installed when it is in the A4 drawer, the A4 drawer's KS-60 access door is secured and the A4 drawer is installed in the equipment rack in the LER. **(T-0)**

3.8.9.3. **[377 TEG Only]**. The KS-60 is properly installed when it is in the A4 drawer, the A4 drawer's KS-60 access door is secured with two Sargent and Greenleaf (S&G) locks, the A4 drawer is installed in the equipment rack in the LER, and launcher closure door is secured with a rail lock or the launcher closure lockpin is secured.

3.8.9.4. Transportation and Handling. All KS-60s listed on COMSEC account 613202 will be issued from the OSB/576 FLTS, transported throughout the missile field and raised and lowered via the appropriate lowering bag. Transport all KS-60s in a hard sided case with sufficient foam padding and Electrostatic Discharge (ESD) protection to prevent damage and meet ESD requirements (ESD protection may be accomplished using ESD type foam or ESD shielding in conjunction with foam protection). **(T-0)**

3.8.9.5. Visual Inspection. Upon issue and turn-in of equipment, all KS-60s will be visually inspected for damage. The inspection will include exterior surfaces, pins, battery hinge, battery holder, etc. for damage beyond normal wear and tear. Minor chips in paint are expected and considered normal wear and tear. **(T-0)**

3.8.10. Command Signals Decoder (Ground) (CSD(G)). The CSD(G) is an electro-mechanical code unit which contains a non-secure arming code which is verified against the non-secure arming code issued by the missile computer. A CSD(G) must be verified on the WCPS before LF installation. WCPS CSD(G) verification paperwork will be maintained in the current LF configuration record. **(T-0)**

3.8.11. OSB COMSEC SIMPLE KEY LOADER (SKL). The AN/PYQ-10C or AN/PYQ-10A (SKL) is an electronic key management system Tier-3 device issued by base COMSEC and is used to load the KIV-7M. These SKLs are governed by COMSEC instruction and maintained by the base COMSEC office. System design requires OSB personnel be designated as SKL Security System Office (SSO) members in order for the WCPS to perform audit data functions.

3.8.12. Data Transfer Unit (DTU). The DTU becomes a critical component at the start of the wing level visual inspection and operational certification (OPCERT) and must be maintained under TPC. Additionally, OPCERT is required before the DTU can be loaded with LFLCD data. The DTU is classified Secret. DTUs used at the 377 TEG will not receive OPCERT and are controlled by classification only. **(T-0)**

3.9. LCC Components. Operations involving LCC code, critical, and miscellaneous components for the MM weapon system are outlined below. For control of code components, reference the EAP-STRAT Vol 16. The MCC will control code components installed in the LCC

and are responsible for proper installation, sealing with holographic TDIs, and removal of all components from the LCC. Proper installation list here do not reference any requirements directed by applicable technical orders for installation of components. Sealing requirements are described in this publication IAW EAP-STRAT Vol 16 and NSA guidance. TDI usage, transport, and storage limitations listed here do not apply to the 576 FLTS. **(T-0)**

3.9.1. LEP. The LEP contains one MCU containing the squadron's J Code. The LEP is classified Top Secret. **(T-0)**

3.9.1.1. Proper Installation. The LEP is properly installed when in the appropriate receptacle within the Rapid Execution and Combat Targeting (REACT) console, installed IAW T.O. 21M-LGM30G-1-24, *Minuteman Weapon System*, electrically mated/verified and sealed with TDIs IAW the EAP-STRAT Vol 16. Failure/inability to tighten all captive screws does not affect proper installation of the LEP, as long as TDIs can be affixed. However, this will be reported and documented as a hardness write-up for the LCC. **(T-0)**

3.9.1.2. Dissipation. For transport of an LEP from the LCC to OSB/576 FLTS, the MCC will contact OSB/576 FLTS for instructions. If a potential compromise situation occurs while transporting a coded LEP, a code handling team will dissipate the code in the LEP by removing the MCU. **(T-0)**

3.9.2. LCP. An LCP contains three MCUs. MCUs A/B form the complete launch code (MCU B also contains an LCC identifier) and MCU C contains the inhibit code. The LCP is classified Top Secret. **(T-0)**

3.9.2.1. Proper Installation. The LCP is properly installed when in the appropriate receptacle within the REACT console, installed IAW T.O. 21M-LGM30G-1-24, *Minuteman Weapon System*, electrically mated/verified and sealed with TDIs IAW the EAP-STRAT Vol 16. Failure/inability to tighten all captive screws does not affect proper installation of the LCP, as long as TDIs can be affixed. However, this will be reported and documented as a hardness write-up for the LCC. **(T-0)**

3.9.2.2. Transport Restrictions. Coded LCPs must be separated by 30 minutes travel time from other LCPs from the same squadron. This restriction does not apply during ECC preparation or when returning superseded and test codes. **(T-0)**

3.9.2.3. Dissipation. For transport of an LCP from the LCC to OSB/576 FLTS, the MCC will contact OSB/576 FLTS for instructions. If a potential compromise situation occurs while transporting a coded LCP, dissipate the launch and inhibit codes by removing all three MCUs (A, B, and C). **(T-0)**

3.9.2.4. Launch Switch Keys. Keys in the LCC will be stored in the LCC Positive Control Material (PCM) container, locked with two locks, to allow one MCCM to enter rest status. These keys will be issued to 576 FLTS personnel who will release the appropriate key(s) as necessary. These keys will not be issued to FDE Task Force personnel. **(T-0)**

3.9.2.4.1. OSB Operations. Code controllers will verify LCP keys by inserting each key (primary and duplicate) into the LCP switch and rotating the keys to ensure both keys and switch work properly. An original and duplicate copy of the LCC Launch Key Verification Record will be completed. Both copies (original and duplicate) of the Launch Key Verification Record will be signed by the two code controllers who

accomplished the verification action. The original Launch Key Verification Record will be laminated and attached to the primary key by code controllers, so it does not interfere with key switch operation when the key is inserted. The duplicate Launch Key Verification Record will be laminated and attached to the duplicate key maintained in OSB. The LCC Launch Key Verification Record will be used by the MCC to verify launch keys match launch switches. The LCC Launch Key Verification Record is attached to the LCP. Launch switches will be verified and sealed with a TDI by code controllers before panels are issued for field use. The classification and LCC assignment will be clearly marked on each panel. **(T-0)**

3.9.3. TSEC/KS-60. The KS-60 contains the active and reserve keys necessary for all encryption and decryption of message traffic within the LCC (Bulk Storage/Loader (BS/L) key) and between the LCC (HICS key) and LF (HICS key). The ITK is a special purpose key for operations requiring the Irreversible Transformation Mode of the KS-60. To mitigate certain threat scenarios, an ITK is required to perform an irreversible transform of launch and enable commands. Only nuclear-certified KS-60s listed on COMSEC account 613202 may be installed at an operational LCC. **(T-0)**

3.9.3.1. Control. An operationally keyed KS-60 is classified Top Secret//CRYPTO//NOFORN. An un-keyed KS-60 is classified Secret//CRYPTO//NOFORN. OSB may direct battery removal of keyed KS-60 for the specific purpose of dissipating electronic key and the KS-60 reverts to Secret//CRYPTO//NOFORN. KS-60s used at the 576 FLTS are not critical components and are controlled by classification only, which is Secret//CRYPTO//NOFORN for FDE missions and Top Secret//CRYPTO//NOFORN for software or communications testing. Reference EAP-STRAT Vol 16 for proper control/handling requirements. **(T-0)**

3.9.3.2. Proper Installation. The KS-60 is properly installed when installed in the Coder-Decoder Assembly (CDA) drawer, the CDA drawer is installed in the REACT console in the LCC and the KS-60 access door and CDA are secured and properly sealed with holographic TDIs IAW the EAP-STRAT Vol 16. **(T-0)**

3.9.3.3. Transportation and Handling. All KS-60s listed on COMSEC account 613202 will be issued from the OSB/576 FLTS, transported throughout the missile field utilizing a hard sided case with sufficient foam padding and ESD protection to prevent damage and meet ESD requirements (ESD protection may be accomplished using ESD type foam or ESD shielding in conjunction with foam protection). **(T-0)**

3.9.3.4. Visual Inspection. Upon issue and turn-in of equipment, all KS-60s will be visually inspected for damage. The inspection will include exterior surfaces, pins, battery hinge, battery holder, etc. for damage beyond normal wear and tear. Minor chips in paint are expected and considered normal wear and tear. **(T-0)**

3.9.4. Weapon System Processor (WSP) and REACT Components. The WSP is the primary processing assembly of the Weapon System Control Element (WSCE). The WSP is a general-purpose digital computer. The function of the WSP is to control the flow of data within and through the LCC. **(T-0)**

3.9.4.1. Proper Installation. The WSP is properly installed when in the appropriate receptacle within the REACT console, installed IAW T.O. 21M-LGM30G-2-12-4, *Missile*

Alert Facility Command and Control Equipment, electrically mated/verified and sealed with TDIs IAW the EAP-STRAT Vol 16. **(T-0)**

3.9.4.2. Code Exposure. In all situations described in the following paragraphs, the MCC will contact OSB for control and handling requirements before allowing a maintenance team to install or remove a WSP drawer or any WSP drawer circuit card(s). These exposures do not apply to the 576 FLTS. **(T-0)**

3.9.4.2.1. C(a)C(b) Control Words Exposure. Control words are exposed upon WSP startup. The components exposed to CMSC control words are the WSP, Coder-Decoder Assembly/Inertial Performance Data (CDA/IPD) interface Circuit Card Assembly (CCA), Coder-Decoder Chassis Assembly and the CDA to WSP Cable Assembly. **(T-0)**

3.9.4.2.2. J Code Exposure. The J Code is considered exposed if the enable switch is off the "SET" position, if the enable switch is in the "DOWN AND LOCKED" position, or if all TDIs sealing the LEP are broken for an unknown reason. Components exposed to the J Code require handling IAW EAP-STRAT Vol 16. Components exposed to the J Code are the WSP, RMB32 circuit cards and the LCP/LEP Cable Assemblies (WV030). **(T-0)**

3.9.4.2.3. Launch Code Exposure. The launch code is considered exposed if the launch key switch is off the "SET" position or if all TDIs securing the LCP are broken for an unknown reason. Components exposed to the launch code require handling IAW EAP-STRAT Vol 16. Components exposed to the launch code are the WSP, RMB32 circuit cards, LCP Interface CCA and LCP/LEP Cable Assembly (WV030). **(T-0)**

3.9.4.2.4. Translate Code Exposure. The translate code is considered exposed when entered via keyboard. Components exposed to the translate code require handling IAW EAP-STRAT Vol 16. Components exposed to the translate code are the Operator Input Device (OID) Keyboard, OID Cable Assemblies (WV019 and WV049), WSP, RMB32 circuit cards and CDA to WSP Cable Assembly (WV015). **(T-0)**

3.9.5. Head Disk Assembly (HDA). The HDA is contained within the BS/L to provide storage of all programs and data. I Codes on the HDA are encrypted. However, a Top Secret-loaded HDA will be controlled two properly cleared couriers when transporting to and from the LCC per DoD Directive S-5210.81, *United States Nuclear Weapons Command and Control, Safety and Security*. Once loaded, the HDA remains classified at the highest level of the data it ever contained until it is destroyed by OSB/576 FLTS. An operational HDA is classified Top Secret. **(T-0)**

3.9.5.1. [377 TEG Only]. A test HDA will be classified based on its highest level of exposure. **(T-0)**

3.9.6. RSM. RSMs are used to update assignments, keys, and code change data files. There are six types of incremental load RSMs: TCI/EPCI, EPP/MA Database, FDM Format Database, code change data, RDCC, and RDCK. An RSM is not a code or critical component but will be controlled based on the highest classification of the data it contains. A Top-Secret RSM will be controlled with two properly cleared U.S. military (or DAFC) couriers when transported to and from the LCC per DAFMAN 17-1302-O, *Communications Security (COMSEC) Operations*. **(T-0)**

3.9.7. OSB COMSEC Simple Key Loader (SKL). The OSB COMSEC SKL is used to load BLACK TEKs and ITKs into the KS-60 at the LCC. RED keys will never be loaded into the OSB SKL. OSB SKLs will be maintained IAW COMSEC instructions. Only the appropriate team may use OSB issued COMSEC SKLs to load BLACK TEKs and ITKs to the KS-60 at an operational LCC. The OSB COMSEC SKL is an UNCLASSIFIED COMSEC controlled item. To support weapon system sustainment the USSTRATCOM will only receive software updates that have been tested and approved by Cryptologic & Cyber Systems Division. **(T-0)**

3.10. Holographic Tamper Detection Indicators (TDIs) (This section does not apply to the 377 TEG). Holographic TDIs are NSA-supplied special purpose holographic labels used on specified LCC equipment to discourage tampering and provide evidence of penetration attempts. Holographic TDIs are used to satisfy TPC for installed LCC components while one MCCM sleeps in the LCC with the blast door closed. The use of holographic TDIs for control of code components is permitted only in the LCC. The unit OSB is the central location for receipt, storage, issue and recovery of holographic TDIs, which will be installed and inspected using the approved DIRNSA/Y2133 procedures. Holographic TDIs will not be used in any other manner without the specific permission of HQ AFSEC/SEWN and the NSA's concurrence. Units will send requests for uses other than those outlined in this chapter to USSTRATCOM through 20 AF/A3NB and AFGSC/A3ON. Units will make requests for changes to holographic TDIs to USSTRATCOM through 20 AF/A3NB and AFGSC/A3ON **(T-0)**

3.10.1. When any panel (except the LCP/LEP) that are required to be affixed with TDIs are removed from the REACT console, a replacement panel must be properly installed and sealed to allow MCCM rest. MCCM rest is not allowed when a panel requiring holographic TDIs is removed leaving an empty hole in the LCC REACT console. If the LCP or LEP cable has not been exposed to operational codes, there is no need for a replacement panel to be installed for these two panels. However, if the LCP key switch has been moved from the SET position or the LEP switch has been moved off the SET position or placed in the "Down and Locked" position, then a replacement panel is required. The MCC will contact OSB for the code status of the LCP and LEP cable prior to removal of the LCP or LEP from the REACT console. **(T-0)**

3.10.2. Operational TDIs and their residue are classified Secret IAW EAP-STRAT Vol 16 until installed in the LCC or destroyed per [paragraph 3.10.4](#) of this publication. In the LCC, uninstalled TDIs may be controlled by one MCCM if they are sealed in cases with other field stored code components or locked in the PC container (with permission of PCM custodian) and the blast door is closed. Training holographic TDIs do not require special controls. Use training holographic TDIs only for training requirements. Uninstalled training holographic TDIs will be secured when not actually being used for training to avoid pilferage. **(T-0)**

3.10.3. The MCC may utilize the LCC PCM container for overnight storage of TDIs with permission from the PCM custodian if PC documents are present. The MCC will notify OSB and Emergency War Orders Flight (OSX) of the requirement for storage and will annotate in the crew log the serial numbers of all TDIs in storage. OSB will also document this storage. Follow normal procedures for authorization to open the LCC PCM container. TDIs may also be stored inside sealed code component cases rather than the LCC PCM container. **(T-0)**

3.10.4. To protect holographic TDI technology, destroy operational holographic TDIs and their residue by cutting them into strips and burning as classified waste. Destroy training TDIs by cutting them into strips lengthwise and disposing of them as Unclassified waste. Unless

directed by USSTRATCOM, bulk destruction (more than 20 at one time) of operational TDIs by units is not authorized. **(T-0)**

3.10.5. Holographic TDI Documentation. All actions involving TDIs will be documented. MCCMs and code controllers (for LCP key switch) will document installation, removal and destruction of holographic TDIs. Questions on how to document operations involving holographic TDIs should be referred to OSB. **(T-0)**

3.10.6. MCCM Rest. MCCM sleep is prohibited if all holographic TDIs on an equipment drawer, a panel, an access door, or a storage case (containing code component(s)) are broken or if the key switch holographic TDI is broken. MCC sleep is also prohibited if all wing holographic TDIs are subject to compromise IAW AFI 91-114. OSB will notify the Alternate Command Post (ACP) of the requirement to terminate MCCM crew rest. When USSTRATCOM evaluation of the Possible Compromise of TDI Technology (PCTT) is complete and it is determined no compromise occurred or all actions in EAP-STRAT Volume 16, Annex A are complete, USSTRATCOM will notify Wing OSB when crew rest may resume. **(T-0)**

3.10.7. Holographic TDI Damage and Breakage. Superficial scratches, nicks, or stains on a TDI that do not prevent it from performing its intended purpose do not automatically require TDI replacement. MCCMs can determine replacement requirements in such instances on a case-by-case basis. Damage and breakage of installed holographic TDIs will be reported to OSB. Breakage of all holographic TDIs on a critical component, code component, or other associated REACT console components or panels that allow access to a code component require an incident report per EAP-STRAT Vol 16 if unauthorized. **(T-0)**

3.10.7.1. Damage to a Holographic TDI. The following situations do not require PCTT, DULL SWORD, COMSEC Incident, or possible code compromise (PCC) reports: holographic TDIs are replaced because they have become marginally acceptable due to superficial scratches or stains; and the inadvertent breaking of a holographic TDI(s) for a known reason when both MCCMs are awake and aware of the cause of the breakage. **(T-0)**

3.10.7.2. Breakage of a Holographic TDI. Notify OSB in all situations concerning the breakage of holographic TDI(s), whether the reason for the breakage is known or unknown or whether the reason for the breakage was authorized or unauthorized. In all situations the damaged or destroyed holographic TDI(s) must be accounted for. **(T-0)**

3.10.7.3. Launch Key Switch Holographic TDI Breakage and Damage Replacement. Notify OSB and request replacement holographic TDIs if the MCC on duty determines a holographic TDI on a launch key switch is damaged or broken for a known reason. MCC rest is not authorized until the launch key switch holographic TDI has been replaced. If both crew members were awake when the damage or breakage occurred, OSB will send a replacement holographic TDI for the launch key switch. In situations where one crewmember was in rest status when the holographic TDI was broken or the damage occurred, the LCP must be replaced due to loss of the launch key switch's integrity. In all situations OSB will determine if the integrity of the LCP key switch is lost and if the LCP requires replacement. **(T-0)**

3.10.8. TDI Installation or Removal. Both MCCMs must be awake during the installation or removal of holographic TDIs from LCC equipment. Installation actions will be accomplished

per EAP-STRAT Vol 16. TDI location in this publication is nominal. Location may be adjusted up to two inches depending on the length and width of the TDI pattern. Removal actions will be accomplished per EAP-STRAT Vol 16. Operational holographic TDIs will only be removed for authorized replacement actions or to support EWO operations. Replacement holographic TDIs must be available in the LCC before initiating any installation or removal action except when the MCC is accomplishing authorized EWO actions. The LCP key switches will be sealed by code controllers prior to issue of the panel. LCPs will be returned to OSB with the key switch holographic TDIs intact. All removed operational holographic TDIs will be destroyed (as classified waste by burning) and destruction of the removed holographic TDIs documented. **(T-0)**

3.10.9. Holographic TDI Inspection. Holographic TDI inspections will be accomplished by the MCCMs who installed the holographic TDIs, each oncoming MCCM during crew changeover, every 24-hour period if a crew change has not occurred, and the MCCMs on duty when possible damage is suspected or detected. Visual inspections will include verification of the integrity of all TDIs, proper installation and placement and pattern verification. Correct fit, form and function of installed TDIs is determined by the MCCM. Inspection details for holographic TDIs are located in Operating Procedures for Rapid Execution and Combat Targeting Tamper Detection for the Intercontinental Ballistic Missile Force provided by NSA. An adjustable high-intensity beam flashlight, with spare light bulbs and batteries, will be available in each LCC for holographic TDI inspection requirements. Unauthorized damage to all holographic TDIs used to secure an LCC-installed critical component or code component may require an inspection of the LCC holographic TDIs by OSB and USSTRATCOM. Questions about the authenticity of a holographic TDI may require an inspection of the installed holographic TDI by OSB and USSTRATCOM. **(T-0)**

3.10.10. Use of Holographic TDIs for Code Component Storage Cases. The use of holographic TDIs for storage of uninstalled, operationally coded panels (and associated uninstalled holographic TDIs) will be limited to periods of Squadron and Worldwide Unlock code changes, SELM tests, or reposturing after major weapon system modifications. Holographic TDIs will be used for SELM test-coded panels. **(T-0)**

3.10.10.1. Major modifications are those operations where work is done by an agency or command other than the using command. **(T-0)**

3.10.10.2. Use the following procedures for securing components in an LCC using holographic TDIs:

3.10.10.2.1. Holographic TDI application will be done by the appropriate code handling team. **(T-0)**

3.10.10.2.2. Affix holographic TDIs to opposite sides of the storage cases not to include the hinged side. **(T-0)**

3.10.10.2.3. Use holographic TDIs only within the LCC. Do not apply seals on the storage case until the coded panel reaches the LCC in which it will be installed. **(T-0)**

3.10.10.2.4. Before installing the holographic TDIs, the MCC will notify OSB and follow their instructions. When components are stored in the LCC, the MCC will log the field storage in the crew log and brief it at MCC changeover. **(T-0)**

3.11. Operation OLYMPIC STEP. Periodic change of operational codes must be performed to ensure compliance with NSA-established code periods. (This section does not apply to the 377 TEG.)

3.11.1. Code Use Period. The code use period begins on the OLYMPIC STEP start date and ends on the date the code is completely removed from operational use. The squadron code use period must not exceed 13 months without prior written approval from USSTRATCOM/J37. Units unable to accomplish OLYMPIC STEP within the above time period must request a waiver through 20 AF/A3NB and AFGSC/A3ON to USSTRATCOM/J37 and DIRNSA/C62. The waiver request letter must include the length of waiver requested in number of days, reason for the waiver, unit(s) affected, current code period start date, 13-month date, and impact if waiver is not granted. DIRNSA/C62 approval is required to extend past the 14-month mark. **(T-0)**

3.11.2. OLYMPIC STEP Dates. 20 AF/A3 and AFGSC/A3O will approve annual OLYMPIC STEP dates after unit coordination. HQ AFGSC will publish approved annual code change dates and immediately provide copy to USSTRATCOM/J374 and DIRNSA/C62. Any changes to the dates will be immediately communicated to J374 and other applicable agencies.

3.11.3. OLYMPIC STEP Planning. Units will coordinate plans internally to concur with projected dates or submit a request for change as required. Unit OLYMPIC STEP must be accomplished in five days or less. In Worldwide Unlock Code Change years, all OLYMPIC STEP actions must be completed either before or after Worldwide Unlock Code change to maximize proper WCPS configuration and to support OSB operations.

3.11.4. Restrictions. All field OLYMPIC STEP actions will cease when any of the following take place in the OLYMPIC STEP squadron: PCC, WSSR violation, or single LCC operations. OLYMPIC STEP actions may resume when the problem is resolved IAW applicable directives. New START coding restrictions are stated at the beginning of this publication. To the maximum extent possible, limit weapon system tests and maintenance not connected with OLYMPIC STEP activities in the affected squadron until OLYMPIC STEP is complete. **(T-0)**

3.11.5. Safety and Control Requirements. Nuclear surety considerations are paramount in determining OLYMPIC STEP sequences and procedures. Special care must be exercised to ensure at least two LCCs with new codes retain the control and monitor functions for all new-coded LFs and at least two LCCs with old codes retain the control and monitor functions for all old-coded LFs. The planned LCC and LF OLYMPIC STEP sequence must be included in each squadron OLYMPIC STEP plan. Single LCC procedures must be implemented immediately if a situation occurs where an LF or LFs cannot be controlled by at least two properly coded LCCs. **(T-0)**

3.11.6. LCC Configurations. A squadron will not enter or continue OLYMPIC STEP activities with less than four operational LCCs. In the event of an LCC shutdown during OLYMPIC STEP or a desire to commence OLYMPIC STEP without the minimum of four LCCs, OSB will notify 20 AF/A3NB who will request a waiver for this requirement.

3.11.7. LCC Preparations. Code components containing the new codes will be positioned at a minimum of three LCCs before the start of OLYMPIC STEP. New components for the remaining LCCs may be positioned after OLYMPIC STEP has started.

3.11.8. Squadron OLYMPIC STEP Sequence. The OLYMPIC STEP sequences and procedures below provide mutual launch and inhibit capability for on-alert missiles during squadron OLYMPIC STEP. The paragraphs below are a recommended sequence of events:

3.11.8.1. LCC Sequence. The squadron OLYMPIC STEP sequence will be for one LCC at a time to load the new BS/L key using the OSB COMSEC SKL and then upload the OLYMPIC STEP code change RSM or install HDA. After all the LCCs have accomplished Local Key Switchover and completed the BS/L key change, LCCs will upload/transmit the REK and ITK to LFs via RDC-K RSM prior to transmitting RDC-C. Always transmit keys before codes. Load new HICS via SKL. Ensure new LEPs and LCPs are installed in at least two LCCs prior to accomplishing remote code switchover.

3.11.8.2. KS-60 Loading Procedures. Only one LCC will accomplish BS/L key change and checksum upload at a time. Ensure that no sole LCC remains on a HICS key during HICS key load if there are LFs still on that HICS key.

3.11.8.3. Accomplish HICS Key switchover IAW TO 21M-LGM30G-1-24.

3.11.8.4. LF Sequence. For the purpose of the OLYMPIC STEP sequence, an LF is considered on new codes once the HICS key has been changed and it is able to be monitored by LCCs on new keys/codes.

3.11.8.5. LF Malfunctions. If OLYMPIC STEP of an LF or LFs is delayed due to malfunction, this delay will be relayed to USSTRATCOM/J374 and AFGSC/A3ON by the unit OSB. USSTRATCOM/J374 will notify DIRNSA/C62 as required.

3.11.9. Old code components and materials will be returned to OSB upon completion of OLYMPIC STEP. Control and handling requirements for all code components remain in force until destruction or disposition.

3.11.10. Units will immediately notify USSTRATCOM/J374 and the JNOC when OLYMPIC STEP is complete or delayed for any reason. The JNOC will notify USSTRATCOM/Global Operations Center, DIRNSA/C62, and AFGSC/A3ON.

3.11.11. Worldwide Unlock (WWU) Code Change. The sequence and procedures outlined below provide mutual enable capability for on-alert missiles during the Worldwide Unlock Code change.

3.11.11.1. A/B Media. Coordinate with USSTRATCOM/J374 to receive new A/B media (with new J Code). Effective time is available in EAP-STRAT Volume 3. **(T-0)**

3.11.11.2. Code Coverage. Retain a minimum of three LEPs (containing old codes) installed in each squadron until the effective time of the new J Code. **(T-0)**

3.11.11.3. Preparation. Code a minimum of three LEPs for each squadron with the new codes. If there are not enough system spares to have full coverage of both old and new codes simultaneously, remove some presently installed LEPs for recoding. Conspicuously label the LEPs containing J codes derived from the new WWU Codes. **(T-0)**

3.11.11.4. Unit Holographic TDI Replacement. All holographic TDIs installed in the LCC will be replaced in conjunction with the unit's Worldwide Unlock Code change. No TDIs containing the replacement pattern will be installed prior to the effective date/time. **(T-0)**

3.11.11.5. Pre-position. Pre-position a minimum of three LEPs (containing new codes) in each squadron. Two LEPs in each squadron will be installed prior to the effective time. Only LCCs with effective codes may perform enabling functions. **(T-0)**

3.11.11.6. Effective Time. At the effective time, all remaining LEPs containing the new codes will be installed. If required, LEPs will be recoded and dispatched to the remaining LCCs as quickly as possible. **(T-0)**

3.11.11.7. Notification. Units will notify the JNOC, and the JNOC will notify USSTRATCOM, DIRNSA/C62, and AFGSC/A3ON when Worldwide Unlock Code change is complete or delayed for any reason.

Chapter 4

CODES VAULT OR SECURE AREA (OSB) OPERATIONS

4.1. Introduction. This section provides organization, training, and equipment management guidelines for ICBM wing codes operations and 377 TEG testing. For control of code components, reference the EAP-STRAT Vol 16. 377 TEG personnel do not maintain code handler status. Certain paragraphs are marked “377 TEG Only” or “576 FLTS/DOX Only”; if not marked, the information herein applies to all operational and test units.

4.2. OSB Daily Operations.

4.2.1. Responsibilities. OSBs and the 576 FLTS/DOX are responsible for the organization, management, and control of the unit’s codes systems. OSBs and the 576 FLTS/DOX will ensure code components, programs, and miscellaneous materials are controlled according to this publication and other guidance. Specifically:

4.2.1.1. Ensure proper configuration of ICBM code and critical components, programs, and miscellaneous devices in support of wing alert readiness requirements.

4.2.1.1.1. **[576 FLTS/DOX Only]**. Ensure proper configuration of ICBM test codes, code and critical components, and miscellaneous materials in support of the FDE and Weapons System Evaluation Program (WSEP) program.

4.2.1.2. Provide timely support for operations, training, and testing activities.

4.2.1.3. Maintain a current and adequate supply of code and critical components, programs, and miscellaneous materials.

4.2.1.3.1. **[576 FLTS/DOX Only]**. Maintain a current and adequate supply of test code components, programs, and miscellaneous materials to support the FDE and WSEP program and lateral coding.

4.2.1.4. Issue to and recover materials from code handling teams.

4.2.1.5. Accomplish coding actions to maintain LCC and LF alert readiness.

4.2.1.5.1. **[576 FLTS/DOX Only]**. Operational code and critical components are not issued to LCCs or LFs.

4.2.1.6. Ensure code and critical components, programs, and miscellaneous materials are controlled according to this publication, the EAP-STRAT Vol 16, and other applicable instructions and directives.

4.2.1.6.1. **[576 FLTS Only]**. Ensure test code components, programs, and miscellaneous materials are controlled according to this publication and other instructions and directives.

4.2.1.7. Provide staff assistance to the commander on codes operations.

4.2.1.8. Prepare and maintain plans required by headquarters directives, including emergency destruction, wing codes operations, and lateral coding.

4.2.1.9. Produce ground, launch, flight, and targeting materials and components for field use.

- 4.2.1.9.1. **[377 TEG Only]**. Produce ground, launch, flight and targeting components to support the FDE and WSEP Program.
- 4.2.1.10. Manage the Code Controller training program.
- 4.2.1.11. Perform SSO responsibilities for OSB COMSEC SKLs used for KS-60 operations.
- 4.2.1.12. Provide SME to operations squadron training sections and provide coordination on products.
- 4.2.1.13. Provide code handler training to maintenance group personnel as requested. 576 FLTS/DOX will provide code handler training to visiting unit personnel for test launches.
- 4.2.2. Duty Restrictions. To ensure maximum safety and security for codes systems, duty restrictions are placed on code controllers. Unlike operational units, there are no duty restrictions for 576 FLTS/DOX code controllers.
 - 4.2.2.1. PCM Custodian. Individuals assigned as code controllers will not concurrently perform PCM Custodian duties. For the one exception to this duty restriction involving translate code operations, see EAP-STRAT Vol 3.
 - 4.2.2.2. Missile Crew Duty. Personnel assigned as code controllers will not concurrently perform missile combat crew duties. An individual decertified as a code controller must not be assigned to missile combat crew duties at the same wing until the launch, enable, penetration, I codes and Worldwide Unlock codes for the same wing and the current TDI pattern (or any TDI pattern to which the code controller had Level 2 access) are superseded. The individual must be decertified as a code controller prior to receipt (by courier or electronic data transfer) of new operational codes. See [paragraph 12.2.1.6.7](#) of this publication for more details. **(T-0)**
 - 4.2.2.3. Enlisted Code Controller Reassignments. Enlisted code controller reassignments must be timed to coincide with OLYMPIC STEP. The individual must be decertified as a code controller prior to receipt (by courier or electronic data transfer) of new operational codes. All codes must be replaced with codes never controlled or handled by the departing enlisted code controller before the individual is reassigned as a code handler. See [paragraph 12.4](#) of this publication and EAP-STRAT Vol 16 for more details. There are no reassignment restrictions for enlisted 576 FLTS/DOX code controllers. **(T-0)**
 - 4.2.2.4. LF/LCC Visit. Any person with access to the WCPS during preparation of operational code data is not permitted unescorted entry to an LCC or LF containing the same data. A code controller, or anyone with access to a CMSC value computed by the WCPS for an operational LF, must not visit the same LF until the CMSC has been obtained at the LF and verified against the WCPS computed number. Code controllers must restrict access to WCPS-computed CMSC values and ensure anyone with knowledge of those values is prohibited from visiting the same LFs until the CMSC is verified. **(T-0)**

4.3. ICBM Wing Coding Operations. For OSB operations involving split-knowledge components, both members of the code controller team will be assigned to the same control group as the component. For split-handled components, at least one member of the code controller team is assigned to the same control group as the code component (e.g., AX or BX). A code component requiring two officer control will be coded and controlled by a two-officer code controller team

(XX). If OSB code controllers are controlling and handling code components outside OSB, both code controllers must be of the proper control group. Refer to EAP-STRAT Vol 16 for required controls of materials.

4.3.1. Two Officer Code Controller Teams. A team composed of two officer code controllers or Department of the Air Force Civilian (DAFC) code controllers of at least GS-7 is used to control those operations involving the following:

4.3.1.1. If the component or operation involves a complete operational launch/translate code (SCPS and WCPS operations/computers, or an LCP).

4.4. Missile Wing and 377 TEG Manning Requirements.

4.4.1. Each OSB and the 576 FLTS/DOX must have enough personnel (officer, enlisted, and DAFC) assigned to provide security, control, and coding support with at least two-officer code controllers (one Group A and one Group B) on a continual 24-hour basis (including standby scheduling and PRP coverage). Nuclear code controllers should be scheduled for duty shifts to ensure this coverage. Staffing must include the capability to provide ongoing AA and BB code controller control for specific OSB functions in addition to normal daily operations. Code controllers on standby must always be available for contact by MMOC or the Command Post, and able to respond within a time specified by the Senior Code Controller/Flight Commander (SCC/FC), along with any additional required personnel, to provide this support. Code controller selectees must have documentation assigning them to OSB prior to WCPS training and are prohibited from handling operational components until certification as code controllers. **(T-0)**

4.4.2. Senior Code Controller (SCC). The SCC is designated by the OSS/CC. The SCC is the Commander's appointed operational leader for OSB. The SCC must be a certified code controller and should have experience and retainability for appointment as determined by the squadron commander. The SCC is ultimately responsible for all COMSEC material, code components, miscellaneous programs, critical components, critical software, and the 20-year spares inventory. He or she must ensure plans are made for proper inventory, control, and accountability of these assets.

4.4.2.1. The Missile Systems Flight Commander (FC). The FC is designated by the 377 TEG /CC. The FC is the Commander's appointed operational leader for the 576 FLTS/DOX and is the SCC for the 576 FLTS. The FC must be a certified code controller and should have experience and retainability for appointments as determined by the squadron commander. The FC is ultimately responsible for all COMSEC material, code components, miscellaneous programs, critical components, critical software, and the 20-year spares inventory. He or she must ensure plans are made for proper inventory, control, and accountability of these assets.

4.4.2.2. Although the SCC and FC are responsible for the overall codes training program, squadron commanders are ultimately responsible to ensure each code handler and code controller has the knowledge and proficiency necessary to properly control ICBM code components, critical components, and miscellaneous material. The SCC/FC monitors the program to ensure the quality and level of instruction meets the needs of the least experienced person and all training is accurate and consistent with regulations and unit requirements.

4.4.2.3. The SCC and FC exercise direct managerial and administrative control over all assigned code controllers and are responsible for the overall unit codes training program. They establish and implement the code controller standardization and evaluation program. By virtue of their appointment, the SCC/FC may conduct training and evaluations. However, he or she must complete all applicable training requirements of the Stan/Eval Officer and Training Officer, commensurate with the task being accomplished.

4.4.3. Chief Operations Officer (OSBO). The operations officer is designated by the SCC/FC and is a certified code controller with experience and retainability for appointment as determined by the SCC/FC and the squadron commander. The operations officer ensures wing coding activities and WCPS operations are performed IAW this publication and Air Force technical orders and instructions. This individual must be knowledgeable of code handling concepts and procedures, OSB and field coding operations and must demonstrate proficiency in WCPS coding and recordkeeping procedures.

4.4.4. Chief Training Officer (OSBT). The Training Officer is designated by the SCC/FC. The Training Officer will be a certified code controller with experience and retainability for appointment as determined by the SCC/FC and the squadron commander. The Training Officer is responsible to the SCC/FC for the management of the unit codes training program, divided into three areas: code handler classroom instruction, code controller classroom instruction, and WCPS instruction.

4.4.4.1. The Training Officer ensures review of all codes related training and evaluation materials prepared by other base agencies to ensure accurate presentation. The Chief Training Officer (or when absent, a designated representative) approves all codes training materials, except as otherwise stated in this document. The Training Officer must ensure annual training is accomplished for the subject areas contained in RCPTM for code controllers and maintenance code handlers. The SCC/FC may appoint the Training Officer to act as program manager and ensure the accomplishment of training activities, but ultimate responsibility rests with the SCC/FC. The Training Officer must continue to meet the requirements mandated by this instruction to maintain active code controller status.

4.4.4.2. **[377 TEG Only]**. The training officer ensures all code controllers are trained IAW this publication and applicable AF and HQ instructions. It is highly desired that appointees have previous training experience in an operational wing or previous instructor experience. The training officer is responsible to the FC for the management of the codes training program. The training officer and/or NCO are appointed in writing by the FC.

4.4.5. Chief, Stan/Eval Codes Officer (OSBV). The Stan/Eval Officer is designated by the SCC/FC. The Stan/Eval Officer is a certified code controller with experience and retainability for appointment as determined by the SCC/FC and the squadron commander. Prior evaluator experience is desired but not required to be appointed to this position. The Stan/Eval Officer must continue to meet requirements mandated by this instruction to maintain active code controller status. 20 AF/A3NB may perform initial certification evaluations of the Stan/Eval Officer to certify as an evaluator, if required (except for the 576 FLTS/DOX). Designated alternate Stan/Eval Officers and enlisted code controllers must meet the same requirements but will only be responsible for the performance of evaluations when needed.

4.4.5.1. The Stan/Eval Officer is responsible for the standardization and evaluation of all training products, operations procedures, operational records, evaluation products, and

conducting personnel evaluations. The Stan/Eval Officer conducts Quality Control Observations (QCO) for the SCC/FC. The Stan/Eval Officer should coordinate with other ICBM unit OSBs to develop standardized practices, techniques, and procedures utilized at their unit where practical.

4.4.5.2. The Stan/Eval Officer validates code controller proficiency by conducting initial and recurring evaluations and ensures the accuracy of coding processes and documentation. The SCC/FC will ensure the Stan/Eval Officer performs an evaluation of the training program and materials to ensure compliance per this regulation.

4.4.5.3. **[377 TEG Only]**. The SCC/FC may also be appointed as the Stan/Eval Officer and can appoint an alternate Stan/Eval Officer or NCO in writing. It is highly desired appointees have previous Stan/Eval Officer or evaluator experience at an operational wing. The Stan/Eval Officer validates code controller proficiency by conducting initial and recurring code controller evaluations IAW this publication and applicable AF and HQ instructions. The Stan/Eval officer also ensures the accuracy of coding processes and documentation.

4.4.6. OSB Flight Commander. The OSB Flight Commander must be a certified code controller in the grade of Captain or above, responsible to the SCC/FC for the supervision of all code controllers. Rank waivers may be granted by 20 AF/A3NB with notification to AFGSC/A3ON. This individual must maintain active code controller status and be knowledgeable of code handler training and the receipt, production, control, handling, storage, recordkeeping, issue, and recovery of code components, operational or test, and whenever possible be an experienced code controller. The flight commander will be responsible for administrative duties and rating on flight members, as well as any other duties as assigned by the SCC/FC.

4.4.7. Superintendent. The Codes Superintendent must be a certified code controller in the grade of Master Sergeant or above, responsible to the SCC/FC for the supervision of enlisted code controllers. Rank waivers may be granted by 20 AF/A3NB with notification to AFGSC/A3ON. This individual must maintain active code controller status and be knowledgeable of code handler training and the receipt, production, control, handling, storage, recordkeeping, issue, and recovery of code components, operational or test. The Superintendent will monitor and assist in the 20-year spares inventory and management of COMSEC materials at their unit which remain assigned to account 613202, as well as any other duties as assigned by the SCC/FC.

4.4.8. COMSEC Responsible Officer (CRO). The CRO is an additional duty assigned to a code controller (certified Department of the Air Force Civilian (DAFC) or active-duty member) responsible to the SCC/FC. The CRO is designated by the SCC/FC for accountability, management, and protection of USSTRATCOM/J374 COMSEC code and critical components and miscellaneous code-related materials at the unit IAW COMSEC instructions and COMSEC managers. The CRO is also responsible for coordinating equipment repair and replacement with the USSTRATCOM/J374 CRO.

4.4.9. Department of the Air Force Civilian (DAFC). Upon assignment and certification, DAFCs will perform duties consistent with their core personnel document and include the responsibilities of an officer code controller as assigned to either A or B control groups.

Additionally, DAFCs are authorized for and qualified to be a member of TPC and two U.S. military member teams.

Chapter 5

FACILITY AND SECURITY REQUIREMENTS

5.1. Physical Description. Each codes office typically contains three main areas: (1) a storage vault or secure area; (2) a Shielded Enclosure (SE); and (3) an office and administration area. The vault or secure area and SE are No Lone Zones and must meet criteria for vaults defined in the DoDM5200.01V3_DAFMAN16-1404V3 and are controlled according to which components are contained within the secure area (also called a secure room) or vaults, IAW EAP-STRAT Vol 16. **(T-0)**

5.1.1. Storage Vault or Secure Area. A room meeting Air Force and NSA standards of a secure room to protect classified information ranging from Confidential to TS//NC2-ESI//CRYPTO, miscellaneous codes-related materials, critical software and components, ICBM code materials (operational & test) and associated equipment. The codes storage area must meet the criteria of a secure area or vault as defined in DoDM5200.01V3_DAFMAN16-1404V3. Code controllers will verify team member PRP certification prior to accessing the secure area or vault containing codes/critical components or sharing combinations to doors and alarm systems to the secure area or vault. Two certified code controllers will satisfy No Lone Zone requirements for the vault or secure area and the area surrounding the SE. **(T-0)**

5.1.1.1. Vault or Secure Area Alarm System. Door(s) must have an alarm system, and the secure area or vault will contain motion sensors that all terminate at a 24-hour centralized alarm monitor station. If a door alarm or motion sensors are inoperative, a TPC team consisting of any two code controllers must guard the No Lone Zone until the alarm is operative. **(T-0)**

5.1.1.2. The vault or secure area must be secured by two changeable combination locks, which must meet Federal Specification FF-L-2740. In addition, one lock must be group 1R as defined in CJCSI 3260.01F, *Joint Policy Governing Positive Control Material and Coded Control Devices*, and DoDM5200.01V3_DAFMAN16-1404V3. This requirement can be satisfied by one of the following methods: **(T-0)**

5.1.1.2.1. A door equipped with two combinations in such a manner both must be worked in order to open the door.

5.1.1.2.2. A door equipped with one lock plus a second lock installed on an inner day gate.

5.1.1.2.3. A door equipped with one lock operating in a dual combination mode.

5.1.1.3. Regardless of the lock option, knowledge of the combinations must be separated with one half controlled independently by Group A certified code controllers and the other by Group B certified code controllers. The combinations used on the door(s) must not be used for any other OSB/576 FLTS/DOX locks. When either lock is inoperative, at a minimum a TPC team consisting of any two assigned personnel must guard the NO LONE ZONE unless there are code components that require specific control in open storage in which case the proper control must be maintained (i.e., LCPs require 2 Officer control). **(T-0)**

5.1.1.4. Control entrance into OSB by using an entrapment area. An entrapment area provides controlled access in and out of the vault or secure area, allows for verification of identity before admittance, permits for summoning of escorts for visitors and provides delay of forced entry. Request a waiver from AFGSC if a current facility does not meet this requirement (this does not apply to 576 FLTS/DOX). Do not allow foreign nationals, unapproved electronic devices, or media entry into the SE or vault or secure areas. **(T-0)**

5.1.2. The Shielded Enclosure (SE) is an electromagnetic/radio-frequency interference-shielded steel room with a sliding, pneumatically sealed door, and provides EMSEC protection for the WCPS and associated equipment. The SE door is audibly and visually alarmed to alert code controllers of EMSEC integrity loss. The SE must be configured so two code controller locks (reference [paragraph 5.5](#) for lock data), one Group A officer control and the other Group B officer control, must be removed to gain entry. When the locks are removed, the SE is controlled by a team meeting both two officer and AB control, except during AA or BB split-knowledge operations (Program Verification System (PVS) Loading or Data Management Device (DMD) battery charging, for example). Individuals not assigned to the wing OSB/576 FLTS/DOX codes flight will not be granted access to the SE without permission of the SCC/FC and will remain under escort. E-Lab technicians are granted escorted access to perform maintenance within the SE. **(T-0)**

5.1.2.1. **[377 TEG Only]**. The SE must be configured so two code controller locks must be removed to gain entry. The combination to one lock is known only by Group A code controllers and the combination of the other lock is known only by Group B code controllers. When the locks are removed, the SE is controlled by any two code controllers. E-Lab technicians will not be given unescorted entry into the SE. **(T-0)**

5.1.2.2. TPC, test and training code components, programs, and miscellaneous materials may be kept in open storage containers within the secure area/vault or SE. Split-handled and split-knowledge operational code components must be stored in split handled or split-knowledge containers in the vault or SE as specified below and IAW EAP-STRAT Vol 16. The vault or secure area must be equipped with containers to satisfy split handling and split-knowledge requirements to support lateral coding IAW [Chapter 8](#). **(T-0)**

5.1.2.3. The SE, storage vault or secure room must have sufficient containers to satisfy split-handling and split-knowledge requirements, equipped with two locks, marked Group A or B. Combinations are known only to the respective certified code controllers. Safes with one lock operating in the dual combination mode meet this requirement. Do not store Group A and B components in the same container. **(T-0)**

5.1.2.4. Group A and B containers will not be open at the same time. Containers will be locked with both locks when the correct code controller team is not present to provide control over the stored code components; this also applies to carrying cases used as storage containers. **(T-0)**

5.1.2.5. Storage containers used for split-knowledge requirements will be kept inside the SE, secured with two locks for the material stored: A1/A2 and B1/B2 combinations on two approved combination locks or individually issued combination locks. Two code controllers of the same group, AA or BB, must be present to grant access to split-knowledge materials. Split-knowledge containers will not be open at the same time. **(T-0)**

- 5.1.2.5.1. **[576 FLTS/DOX Only]**. Storage containers used for split-handling requirements will be kept inside the SE, secured with two locks for the material stored: A and B combinations on two approved combination locks or individually issued combination locks. **(T-0)**
- 5.1.2.6. Code components, critical components, programs, and miscellaneous materials will be kept in the secure area, storage vault or SE as follows:
- 5.1.2.6.1. Code components which do not require split handling may be kept in open storage.
- 5.1.2.6.2. Two officer control components may be stored in open storage only in the SE (e.g. an operational WCPS computer). KS-60 operations require split-knowledge operations (AA and BB) during PVS key loading. During these operations ensure split-knowledge control teams meet all requirements for components present in the SE. **(T-0)**
- 5.1.2.6.3. MGS parameter data, target, and execution materials and TDIs may be stored in the vault, secure area or SE.
- 5.1.2.6.3.1. **[377 TEG Only]**. MGS Parameters CDs are Unclassified once received for a test launch; however, the CDs are maintained until after the launch is complete. The media can be destroyed when codes dissipation approval has been received from all 377 TEG agencies. Media for backup guidance sets are retained until needed or released to maintenance teams for shipment.
- 5.1.2.6.4. Test code components. Test code components may be stored with their corresponding operational components; however, they must be conspicuously marked to distinguish them from operational components. **(T-0)**
- 5.1.2.6.4.1. **[377 TEG Only]**. Test code components may be stored in open storage in the SE or the vault or secure area. A non-code code controller TPC team (e.g., E-Lab) will not have unescorted access to the vault unless all code components are secured in the SE. PVS and WCPS Key CDs require split-handling control and must be stored IAW the guidance specified in [Chapter 5](#). **(T-0)**
- 5.1.2.7. All units will maintain an Uninterruptible Power Supply (UPS) in support of the WCPS. Due to the rarity and critical nature of this equipment, it will not be exposed to the dangers of unfiltered power, brownouts, blackouts, etc. Additionally, all facilities containing a WCPS will be supported by a backup generator to allow sustained mission support. **(T-0)**
- 5.1.2.8. Provisions must be made for emergency lighting to ensure proper control of the storage vault and SE during power failures.
- 5.1.2.9. Units will develop a plan to ensure notification of planned and unplanned commercial power losses affecting buildings where a codes vault is located or where code components are being stored.
- 5.1.2.10. If a building where a codes vault is located or where code components are stored experiences a total power loss to the security system, regardless of UPS status, the vault or area containing code components must be guarded by two qualified code controllers until

power is restored. When power is restored, a functional check of all alarms must be performed. **(T-0)**

5.1.3. Shielded Enclosure Tempest Recertification. The SE requires TEMPEST recertification every 3 years per the AFSSI 7702 (Air Force Systems Security Instruction). It must be tested according to the NSTISSAM/TEMPEST 1-95 standards. AFGSC/A3O will work with the AFNWC/NIMY (ICBM Program Office), 20 AF, and the AF Certified TEMPEST Technical Authority (CTTA) to ensure the SE goes through the recertification process, to include all needed repairs and pretests. The results of the TEMPEST test will go through the AF/CTTA for review and acceptance or denial of test results. If a TEMPEST recertification test fails the AF/CTTA can provide temporary TEMPEST exception up to one year. Any waivers exceeding 1 year will require deliberate risk acceptance. AFGSC/A6Q will coordinate a risk acceptance package for AFGSC A6 decision. The risk acceptance package should contain a memo detailing the risks being accepted including radio frequency test results and any risk acceptance recommendations from AFNWC/NIMY. Final routing for TEMPEST and Weapons system specs results will be collected by A3ON, coordinated through AFNWC/NIMY and AFGSC/A6Q and then administratively routed to A6 for decision. If AFGSC A6 accepts the risk it must be coordinated in writing through the CONAUTH (CDRUSSTRATCOM or delegated individual) to the Joint Staff, J-3 IAW CJSCI 3260.01F.

5.1.4. Office Area. All assigned code controllers and administrative specialists may share keys or combinations to office areas outside the vault area as approved by the SCC/FC. When the vault door is open or insecure, the No Lone Zone encompasses the office area and extends to the exterior doors.

5.1.5. No Lone Zone. The vault or secure area and SE are designated No Lone Zones; the SE is not an exclusion zone. Access to the codes storage vault or secure area is controlled by any two TPC-certified code controllers; E-Lab personnel will not have access to the vault or secure area until it has been opened by two code controllers. An TPC certified E-Lab technician team satisfies TPC requirements and may be used to fulfill No Lone Zone requirements of the storage vault or secure area to perform HCVE maintenance activities provided all code components are locked inside storage containers, or the SE and two code controllers can monitor and detect unauthorized entry to the SE. **(T-0)**

5.1.6. Entry Security. Do not allow foreign nationals or media entry into the codes vault or secure area. All individuals not assigned to OSB/576 FLTS/DOX will be properly identified and their requirement to enter validated before permitted entry to No Lone Zone(s). Anyone other than local code controllers and E-Lab TPC team members who enter No Lone Zones will be always escorted by a code controller team. Non-DoW personnel will not be allowed access to critical/code components and other related devices without approval from the OSS Commander and concurrence from USSTRATCOM/J374. An exception to this is the Contractor Logistics Support and contractor support personnel who perform troubleshooting actions, modification programs and periodic maintenance inspections on the WCPS; those visits are coordinated in advance. Photography and multimedia recordings of code facilities, equipment, LFs, LCCs, and test launch processes are determined by the SCC/FC in consultation with the squadron commander or 377 TEG Commander or Director of Operations IAW instructions provided in 20 AFI 31-133, Attachment 11. Maintain a log of all non-wing visitors in the vault or secure area for a period of one year. The visitors log will include the name, organization, date/time, and reason for the visit for each visitor. **(T-0)**

5.1.6.1. Non-PRP Visitors. If a visitor requires vault or secure area access while no coding operations are in progress, one member of the TPC code controller team may act as an escort if there is no coding or maintenance being performed.

5.1.6.2. If a visitor requires vault or secure area access during coding operations, code controllers must ensure the visitor is escorted within the SE by a single, dedicated escort official who is properly cleared for coding actions. The code controller team performing coding actions cannot perform escort duties. As the TPC team controlling the SE, they must ensure the escort and visitors are always within sight. Ensure the area where visitors are present is sanitized of classified material to the correct clearance level. **(T-0)**

5.1.6.3. If a visitor requires access during unit-conducted training or evaluation of coding operations, code controllers must ensure the visitor is escorted within the SE by a single, dedicated escort official who is properly cleared for the coding actions. Neither the code controller team nor the instructor or evaluator can perform escort duties. The code controller team performing the coding actions, as the TPC team, will ensure the escort and visitors are always within sight.

5.1.6.4. Code controllers must keep visitors into the SE at an absolute minimum, especially during coding operations. More than two visitors at a time should only be allowed on a case-by-case basis and only for exceptional reasons. The SCC/FC makes the final determination for allowing secure area, vault and SE access.

5.1.6.5. All OSB tours will be approved by the SCC/FC. During coding operations, tours of the OSB vault or secure area will be limited to individuals who are not currently CMR or projected or scheduled to be CMR and have a valid “need-to-know”.

5.2. Reports. Each OSB will submit the following as required:

5.2.1. Monthly code controller listings, certifications, and de-certifications of code controllers to USSTRATCOM/J374, AFGSC/A3ON, and 20 AF/A3NB.

5.2.2. Monthly OSB and USTRATCOM/J374 equipment and WCPS anomaly reports to AFGSC/A3ON and 20 AF/A3NB.

5.2.3. Annual Master Lesson Plans (MLP) to 20 AF/A3NB IAW this publication and at each revision of the USSTRATCOM EAP-STRAT Volume 16 and/or this instruction. 20 AF/A3NB will document approval and all reviews and maintain this documentation with the MLP. At a minimum, MLPs must identify JPRs to be trained, the associated learning objective, and how to meet said objective.

5.2.4. Deficiency Reports to 20 AF/A3NB, AFGSC/A3ON, USSTRATCOM/J374, and DIRNSA/C62 as needed, IAW Section 1, Chapter 9 of this publication. **(T-0)**

5.2.5. Dull Sword Reports are made to Wing SEW IAW DAFI 91-204 separately but in conjunction with PCC reports as required. The details of a PCC are Secret and Dull Sword Reports containing the same information as the PCC will be made via secure means. **(T-0)**

5.3. Deactivation Plans. Each OSB will ensure LF and LCC codes are removed IAW all applicable and approved unit deactivation plans. Follow LF penetration guidance in this document in cases where code components are improperly installed at an LF undergoing deposture. In the LCC, panels pulled during deposture do not need to be replaced provided code-exposed components (if any) are also removed or access to code-exposed components (if any) is controlled

by the proper code handling team. Furthermore, MCCM rest is permitted in capsules undergoing deposture where panels previously sealed with TDIs are removed provided code-exposed components (if any) are removed as well. If code-exposed components remain, two MCCMs must remain awake unless a replacement panel or cover plate is installed and sealed with TDIs. **(T-0)**

5.4. WCPS Coding Management Guide. 20 AF/A3NB will provide the WCPS Coding Management Guide to all units. Updates and feedback are requested via email correspondence to 20 AF. Reviews of procedures will be conducted at least annually or when technical order changes necessitate a review to ensure currency of the information and references. 20 AF/A3NB will notify AFGSC/A3ON of any changes to the guide. AFGSC/A3ON will then up-channel the changes to AFGSC/IG for inspection purposes.

5.5. Locks. Locks are controlled in such a manner as to preclude unauthorized disclosure of the lock's combination. The combination for each lock will be changed at least every 6 months, whenever an individual knowing a combination is decertified, when a combination has been compromised, or when maintenance has been performed on the door or lock. Combinations will consist of three different numbers followed by zero. Use of single dial, three position, changeable combination padlocks (NSN 5340-01-562-6775) is authorized. **(T-0)**

Chapter 6

CODING EQUIPMENT AND MATERIALS

6.1. General. Each OSB must maintain code components, data, and materials ready for dispatch in serviceable condition. Protect all code materials and media from adverse environments (i.e., excessive heat, cold, moisture, shock, vibration, electromagnetic radiation hazards) to the maximum extent possible. Store all WCPS media and spare media inside the SE. Store all coding material, supplies and equipment authorized for use by this and other instructions to support code controller duties within the confines of OSB.

6.1.1. **[377 TEG Only].** Specific FDE and WSEP support test code equipment and material must be on hand as determined by the SCC/FC and commander to meet mission requirements.

6.1.2. Maintain a minimum spare inventory of five LCPs, five LEPs, five CCVs, five KS-60s, five HDAs, and fifteen OSB COMSEC SKLs in serviceable condition to support routine and emergency coding requirements.

6.2. Component Dispatch, Recovery and Team Briefings.

6.2.1. Issue code components and perform operational coding on the WCPS when required by technical orders or maintenance procedures. “What if” or “just in case” coding to prepare for simultaneous maintenance procedures is not permitted. KS-60 key management provides the ability to code replacement KS-60s as needed to support troubleshooting and is not “just in case” coding.

6.2.2. Equipment prepared for dispatch must be in serviceable condition and include all required hardware (batteries, fuses, fasteners, etc.). Items recovered from courier teams must be serviceable or have discrepancies documented for required corrective action. Serviceable carrying cases will be used for transporting all coding materials. Tools for removing MCUs will be issued to code handling teams who receive and transport LCPs and LEPs.

6.2.3. Master media and WCPS-dedicated CDs will not be issued from OSB. Do not simultaneously issue complementary operational PEN C and PEN D data from OSB. **(T-0)**

6.2.4. Code Controllers must verify coding requirements with local maintenance schedules or the MMOC. Code controllers will identify all dispatching team members using personal recognition or military identification cards prior to entry into OSB or issuance of a critical or code component. Ensure all members of the code handling team have their code handlers status verified prior to issuing material from OSB.

6.2.5. If a code handling team must transfer components to another team in the field, the team chief will notify OSB prior to field transfer.

6.2.5.1. When conducting a field transfer, the transferring team chief must identify the receiving team members via personal recognition or by checking the receiving team members’ military identification cards. The transferring team chief will ensure each team members’ code handler status is verified with OSB prior to transfer. **(T-0)**

6.2.5.2. Field transfer of OSB-issued materials will occur at the LF or MAF; exceptions are approved only by OSB. During field transfer, both transferring and receiving teams must be in a position to hear the transfer briefing via telephone or radio.

6.2.5.3. After OSB verifies a team's code handling status and provides a handler briefing for the team assuming responsibility for the components, notify the affected missile crew of the field transfer.

6.2.6. Any teams performing tasks affecting the physical security of code components or handling, receiving, controlling, or transferring OSB-issued materials must be briefed by OSB code controllers before dispatching to the LF or LCC or performing any task involving those materials. All code handler team members must receive this briefing. Briefings will cover the information needed to ensure proper control of item(s), to include minimum team controls, transport, field transfer and storage, documentation, emergency destruction, reporting requirements, and duress words. Tailor the briefing to local needs or requirements based on SCC/FC recommendations.

6.3. Transfer and Shipping of COMSEC and Codes-Related Materials.

6.3.1. A code controller team (AB) will receive and/or transfer COMSEC account 613202 shipments or other code-related material on a *DD Form 2825, Internal Receipt*. This team will transport the package(s) between the transfer point and OSB. **(T-0)**

6.3.2. Upon return to OSB, a code controller team of the proper control group (as indicated on shipping documents) will inventory and sign receipt for the items on the enclosed *Standard Form (SF) 153, COMSEC Material Report* filled out as a hand receipt. The code controller team will sign one SF 153 to return to USSTRATCOM/J374 within 5 working days and retain the other to hold in OSB's files until the item appears on the Unit Master Record (UMR). Report discrepancies immediately to USSTRATCOM/J374. **(T-0)**

6.3.3. USSTRATCOM/J374 must approve the transfer of all COMSEC account 613202 materials between units. Document transfers with an SF 153 completed as a hand receipt. The sending unit prepares four copies and places three copies inside the package and retains one copy until the item(s) no longer appear on the UMR. The receiving unit signs all three copies after receipt and inventory; returns one copy to the sending unit; sends one copy to USSTRATCOM/J374; and files the last copy until the items appear on the UMR. **(T-0)**

6.3.4. When returning packages to USSTRATCOM/J374, document the transaction using three copies of the SF 153 completed as a hand receipt. Include two copies in the package and retain one copy in OSB records. USSTRATCOM/J374 will sign and return one copy of the hand receipt. Replace the first copy in OSB records with the signed copy and retain until the items are removed from the UMR. The transfer and inventory of target execution materials and other classified materials that are not COMSEC items will be accomplished IAW AFGSC and Air Force instructions. **(T-0)**

6.3.5. COMSEC materials will be packaged and shipped IAW TO 00-33B-5508, *Control and Handling of ICBM Minuteman COMSEC Material*.

6.3.5.1. Code components and other critical components that cannot be decertified or recertified must be controlled by a code handling or TPC team, depending on the material being shipped. DAFI 91-101 authorizes use of the Defense Courier Service (DCS) for shipment of critical components under certain circumstances. TDIs cannot be used on shipping containers and DCS couriers do not meet TPC requirements. Therefore, certified code or critical components may not be shipped using DCS couriers. This restriction does

not apply if a component can be decertified and later recertified or is not operationally certified. **(T-0)**

6.3.5.2. Teams used for courier duties must meet the handling and control requirements for the material being transported. OSB/576 FLTS/DOX will brief all team members on their control responsibilities and provide a courier designation letter with written instructions. **(T-0)**

6.3.5.3. A courier letter must contain the full name, rank, and DoW ID number of all courier team members; the effective time period of the transportation (include additional days in the event of travel delays); a home station POC and phone number; classification and control of material; number, approximate size, and type of packages transported; a statement exempting the package from x-ray or physical examination; and transportation instructions specific to the material (if required). **(T-0)**

6.4. Component Markings. Critical components issued by OSB will be marked “TPC Team”. If a critical component is issued and transported in a carrying case, only the carrying case need be marked. If a critical component is issued and transported without a carrying case, the component itself must be marked. Code components and carrying cases will be marked to indicate special code handling team requirements (XX/Two-Officer) when transported outside the vault or secure area. Coding materials will be conspicuously marked by a labeling method not interfering with the handling or operation of the component. 576 FLTS/DOX will mark components and cases with the actual controls/classification of the test material being transported.

6.4.1. Critical components stored inside the vault or secure area are not required to be marked. Any required markings and information will be attached using removable tags. No other markings are authorized.

6.4.2. Code components will be clearly identified with a control number IAW EAP-STRAT Vol 16. **(T-0)**

6.4.3. All components will be marked to indicate classification, identifying control number, copy numbers (if applicable), WCPS, squadron, LCC, or LF assignment (P-Plugs excluded). **(T-0)**

6.4.4. The assignment, classification and any applicable special handling notations will be clearly indicated on all WCPS-produced media. Coding media will have identification labels (do not use raised lettering labels) affixed to the CD. **(T-0)**

6.4.5. All classified materials, excluding CRYPTO items, must be marked with downgrade or declassification instructions. Code components produced by NSA or derived from components produced by NSA do not require downgrade or declassification instructions. **(T-0)**

6.5. Inventories. All code and critical components, programs, and miscellaneous materials in OSB/576 FLTS/DOX will be inventoried within the intervals specified below. Teams conducting inventories must meet control requirements for the components inventoried. OSB/576 FLTS/DOX will maintain periodic inventories for three (3) years. **Note:** AA/BB inventories must be signed by the personnel who performed the inventory.

6.5.1. Every 15-days, inventory the following: all operationally coded LFLCDs, DTUs containing LFLCD data; launch or enable-coded equipment (LCPs, CCVs, LEPs, WCPS computers, WSP cards). The 576 FLTS/DOX does not conduct 15-day inventories.

6.5.2. Every 30 days, inventory the following: all master media; encrypted CDs and disks; CTUs (if applicable); PEN D LFLCDs; DTUs containing Pen D LFLCD data, uncoded or training data coded DTUs; DMDs; KS-60s; reserve and superseded P-Plugs; Key CDs; OSB COMSEC SKLs; USWAA-61 parts A/B; USWAR-61 parts A/B; failed or damaged circuit cards; test and training code components; duplicates of operational launch switch keys.

6.5.3. Every 90 days, inventory the following: all programs; MGS Parameters CDs; TDIs not in bulk storage; uncoded LCPs and LEPs; PROM Fuser Verifiers; CCV good and faulted ROM cards; all targeting and execution program and database media; KIV-7Ms.

6.5.4. Semiannual inventories will include all WCPS 20-year spares. These may be inventoried in bulk. When a spares program manager changes, a physical inventory of all spares (opening and inventorying of all bulk packages) is required prior to the new spares program manager assuming responsibilities for the program.

6.5.5. When units receive an updated UMR from USSTRATCOM/J374, verify those materials are correctly listed and on-hand. The UMR inventory – a physical inventory of the listed materials or a cross-check of the listed materials against LF or LCC installation records – is accomplished by two code controllers of the appropriate control group. COMSEC account 613202 materials not listed on the UMR will be added to the list. Notify USSTRATCOM/J374 immediately of UMR discrepancies. A signed copy of the UMR will be returned to USSTRATCOM/J374 within five working days of receipt. If any individual who signed the last posted UMR departs the unit, the UMR must be re-accomplished. This will release the previous individual of any accountability for the material listed on the UMR. **(T-0)**

6.5.6. All SCC/FC selectees will conduct a 15-, 30-, and 90-day inventory; an inventory of all items listed on the UMR; and a physical inventory of WCPS 20-year spares prior to assuming SCC/FC duties. Opening of bulk packages is not required for 20-year spares unless completed in conjunction with a program manager change. Items installed in the LCCs and LFs can be verified with a 100 percent audit of LCC and LF installation paperwork by the SCC/FC selectee. Results of these inventories will be documented and filed in OSB/576 FLTS/DOX records and with the SCC/FC appointment letter. OSBs/576 FLTS/DOX will send 20-year spares inventory reports to 20 AF/A3NB. 20 AF/A3NB will forward those reports to AFGSC/A3ON and AFNWC/NIAG.

6.6. Failed or Broken Items. Failed or broken code or critical components and miscellaneous coding equipment will be reported by OSB576 FLTS/DOX IAW DAFI 91-204, *Safety Investigations and Reports*. If AFGSC or USSTRATCOM/J374 furnished program or miscellaneous media is damaged, request a replacement from AFGSC or USSTRATCOM/J374, as applicable, via memorandum and include the media number and part number. Destroy the damaged media after its replacement arrives. **(T-0)**

6.7. Asset Tracking. OSB/576 FLTS/DOX will maintain a tracking system for USSTRATCOM assets and will label and classify documents and materials IAW USSTRATCOM directives. **(T-0)**

6.8. Documentation. Access to any document which is classified or unclassified identifying operational codes will be strictly limited to personnel directly involved in the management, maintenance, evaluation, inspection, and operation of the Minuteman secure code system. All forms, records, and other documents used by code handling teams during field coding operations

will be strictly controlled and returned to OSB/576 FLTS/DOX immediately upon return to base. (T-0)

6.8.1. Documentation duplication. LF and LCC records will not be duplicated. LF and LCC records will not be stored outside the confines of OSB/576 FLTS/DOX. Whatever local benefits may be derived from doing so do not outweigh the increased risk of compromise which could potentially lead to the re-coding of the entire nuclear force (ICBMs, bombers, and submarines). (T-0)

6.8.2. Destruction. Unclassified forms, records, listings, or documents having been superseded will be disposed of as classified waste. Erroneous or incomplete forms, records, listings, or documents replaced with correct or complete counterparts are not required to be placed in the inactive section. They will be destroyed as classified waste.

6.8.3. Issue and Recovery of Code Handling Paperwork.

6.8.3.1. Issue of Code Handling Paperwork. The issuing code controller team will review the proper recordkeeping procedures to be completed during coding operations or installation of a code component with the dispatching code handling team.

6.8.3.2. Recovery of Code Handling Paperwork. The recovering code controller team will review the completed code handling paperwork with the code handling team. Any errors or questions about what the code handling team accomplished during coding operations or code component installation or removal will be corrected or answered before the team is released from their code handling responsibilities.

6.8.4. Code Operations Log. The Code Operations Log will be maintained daily. A single operations log may be used to cover weekend and holiday shifts. The log should provide sufficient detail for significant events to be reconstructed. The following information will be entered into the log: duty code controllers, issues, and recoveries, WCPS coding action (operational and training), inventories, alarm checks, CMSC and VN verifications, and receipt and delivery of codes and codes-related materials.

6.8.5. Document equipment failures or discrepancies of USSTRATCOM/J374-owned equipment/COMSEC items (i.e., KS-60) IAW T.O. 00-20-3, *Maintenance Processing of Repairable Property and the Repair Cycle Asset Control System*, and by memorandum or email to USSTRATCOM/J374, with a courtesy copy to 20 AF/A3NB, for corrective action. Ensure the appropriate tags are affixed to each equipment item reflecting the specific issue. (T-0)

6.8.6. Documents for Simulated Electronic Test Launches (SELM). Documents for SELM will be made available to military or contractor personnel when coding verification, failure analysis, etc., is required. These documents should be screened before release to ensure operational information is properly controlled.

6.8.7. WCPS Printouts. The WCPS printouts are used to record data used or produced during coding operations. A code controller team of the proper control group will certify and sign each printout used to document a coding action. As a minimum, a coding action is defined as a coding procedure for which WMAP has a recordkeeping function. Comments can be added (either in pen or by using the comment feature (C*) of the WCPS) to add any remarks deemed necessary by the code controller team.

6.8.8. WCPS-computed SCSC and CMSC controls:

6.8.8.1. Within five working days of receipt of A and B media data, code controllers will produce primary A and B media and verify SCSC with the USSTRATCOM/J374-provided SCSC letter. After successful verification, code controllers may use the provided code data. Notify USSTRATCOM/J374 by telephone if verification fails. **(T-0)**

6.8.8.2. CMSCs are computed to ensure the proper load of complete load data. A CMSC is invalid if no CMSC, an incomplete CMSC, or any CMSC other than the one computed on the WCPS is obtained following a DTU load. These conditions are the result of equipment malfunctions, personnel error, or an unauthorized act.

6.8.8.3. In the event of an invalid CMSC, code controllers will: 1) verify with MMOC the correct actions in Section 1 were accomplished; 2) perform CMSC backout procedures IAW applicable technical orders; 3) investigate the situation to determine if an unauthorized act caused the invalid CMSC.

6.8.8.4. If equipment malfunction or code controller error caused an invalid CMSC, DTUs with LFLCD data can be issued to the maintenance team which obtained the invalid CMSC provided the proper control is maintained for complementary PEN C and D data. In all other cases, a different maintenance team must be used to accomplish the LFLCD load.

6.9. LF Components.

6.9.1. P-Plugs contain the LF unique portion of the launch code. The control date is the date it arrives at OSB.

6.9.1.1. Store P-Plugs in split-handled containers of the appropriate control group in the storage vault or SE. Superseded P-Plugs awaiting destruction must be stored separately from P-Plugs awaiting installation or unassigned. **(T-0)**

6.9.1.2. P-Plugs will not be issued to the field until the data is read from the P-Plug into the WCPS and verified to be identical to the corresponding data on Master N media. Always perform the exclusions test when loading P-Plug data into the WCPS. OSB will make two backup copies of the data disk after loading P-Plug data. **(T-0)**

6.9.1.3. P-Plugs that fail to load on the WCPS will be transferred to USSTRATCOM/J374 for return to NSA for analysis. Conspicuously mark failed P-Plugs and store separately from unused or superseded P-Plugs. Send a SIPR email identifying the failed P-Plug(s) to USSTRATCOM/J374, with information copies to 20 AF/A3NB, AFGSC/A3ON, and DIRNSA/C62. **(T-0)**

6.9.1.4. Operational P-Plugs are only used once. A P-Plug change is required anytime a P-Plug used in an LF CMSC computation or attempted computation, is removed from its MGS, or the MGS containing the P-Plug is removed from the LF fenced area. Certain exceptions to this rule are included in CMSC backout procedures in T.O. 31X8-2-2-1. **(T-0)**

6.9.1.5. Retain superseded, damaged, or failed P-Plugs until transfer to USSTRATCOM/J374. Mark P-Plugs according to condition (superseded, damaged, failed, awaiting destruction) and package them without Styrofoam. USSTRATCOM/J374 will transport P-Plugs to DIRNSA/C62 for disposition. **(T-0)**

6.9.1.6. **[377 TEG Only]**. Test P-Plugs are CUI//CRYPTO items and are stored in the vault, secure area, or SE. Exclusions tests are not necessary when loading P-Plug data into

the WCPS. The control date is the date it arrives in the 576 FLTS/DOX. Upon launch or destruction, the P-Plugs are deleted from the codes database; request USSTRATCOM/J374 update the UMR accordingly. P-Plugs may be reused for MGS changes as needed. P-Plugs destroyed during Operational Test Launches will be documented on SF 153 and this documentation will be provided to USSTRATCOM/J374 as soon as possible. **(T-0)**

6.9.2. LFLCD: A Complete Load LFLCD contains PEN data, OGP/OFP, flight constants and MGS Parameters data and is used to load data into the MGC. A Complete Load LFLCD is classified Secret//CRYPTO. PEN D LFLCD data contains PEN data to unlock the MGC for local overwrite. It is classified Secret//CRYPTO. Control dates for LFLCDs will be the date of creation on the WCPS. **(T-0)**

6.9.2.1. Do not simultaneously issue LFLCDs containing complementary PEN C and PEN D data. **(T-0)**

6.9.2.2. LFLCDs that are incomplete, damaged or that fail to load or verify must be controlled and destroyed using an NSA-approved destruction device. **(T-0)**

6.9.3. DTU: The LFLCD data is loaded to the MGS at the LF via a DTU, and a DTU may contain data for up to 12 LFs.

6.9.3.1. Do not load a DTU with more than one LFLCD containing the standard engineering file ("Dummy File"). **(T-0)**

6.9.3.2. Do not simultaneously issue DTUs containing complementary PEN C and PEN D data. **(T-0)**

6.9.3.3. Whenever the DTU is issued to the E-Lab technicians, the LF data must be erased by OSB code controllers. A briefing on DTU TPC controls must be given when a non-coded DTU is issued. **(T-0)**

6.9.3.4. The spare and removed Processor Circuit Cards will be stored in OSB. **(T-0)**

6.9.3.4.1. These circuit cards must be carefully stored as TPC items, until needed for use in the DTU, and to prevent damage from static electricity. **(T-0)**

6.9.3.4.2. Disposition. The DTU Processor Circuit Card must be removed and replaced with a certified Processor Circuit Card whenever loss of TPC of a coded or uncoded DTU occurs. Processor Circuit Cards removed due to a loss of TPC will be retained in OSB until shipment to USSTRATCOM/J374 under TPC can occur. These circuit cards must be carefully stored to prevent damage from static electricity. **(T-0)**

6.9.3.4.3. Damaged or failed DTU processor circuit cards can be returned to the supply system as Secret//CRYPTO items for shipment to depot. **(T-0)**

6.9.3.4.4. **[377 TEG Only]**. DTUs are classified Secret//CRYPTO. Operational certification of the DTU is not required at the 576 FLTS/DOX. **(T-0)**

6.9.4. Code Change Verifier (CCV): A CCV and its output cable become critical components at the start of their initial functional certifications at an operational unit until they are released by the OSB for non-operational use. The control date of a CCV will be its encoded date on the WCPS. The CCV cables will be conspicuously marked with its corresponding CCV number. **(T-0)**

6.9.4.1. Store all CCVs in split-handled containers of the appropriate control group in the storage vault or SE. **(T-0)**

6.9.4.2. All CCVs used to insert or remove a code must be verified using the WMAP Verify CCV procedure. If the verification of a CCV used to insert an operational code fails, remove, and withhold the missile from alert and apply operational controls until a successful verification is achieved. If the verification of a CCV used to remove an operational code fails, apply operational controls to the affected missile(s) until a successful CCV verification is achieved. CCV trace data will be printed immediately after unloading the data onto the WCPS data disk. **(T-0)**

6.9.4.3. VNs are computed by the WCPS for each CCV encoding operation. The CCV will display the VN after successful transfer of the enable code. Once the VN is validated by one code controller, unit command post or MMOC controller, the missile may be called on alert. An invalid VN (no number or a number other than the WCPS-computed VN for LF) requires dispatch of a second CCV if OSB cannot verify VN IAW T.O. 31X8-2-2-1. A CCV re-verify error as listed in applicable maintenance directives will allow the sortie to be called on alert after OSB verifies the CCV and reviews the trace data for the indicated error. The same team performing the original coding operation may be used for the second dispatch unless an unauthorized act is suspected. A PCC will be declared if unauthorized acts are determined to be the cause of an invalid VN. **(T-0)**

6.9.4.4. CCV Good and Faulted ROM Cards. Each OSB will maintain at least two certified Good and Faulted ROM cards for use by E-Lab. E-Lab uses a Good and Faulted ROM card to certify their Program Memory Comparator (PMC). The PMC, in turn, is used to certify CCVs. The OSB will recover the cards after use by E-Lab. If TPC control of a Good and Faulted card is lost, the card will be returned to AFGSC for recertification. **(T-0)**

6.9.4.5. CCVs can be administratively decertified after all operational codes processed by the CCV are superseded, or after removal of the Code Storage Element (CSE)/PROM (U36) from the CCV printed wiring assembly. The CSE/PROM is classified and must be controlled after removal. The signal cable can be administratively decertified after code supersession. **(T-0)**

6.9.4.6. **[377 TEG Only]**. Test coded CCVs are Unclassified. The control date of a CCV will be its encode date on the WCPS. Store all CCVs in the codes vault or SE. If the CCV fails verification or the VN received from the team is invalid, withhold the missile from simulated alert or launch until a successful VN is achieved. **(T-0)**

6.9.5. CSD(M). A CSD(M) is an electro-mechanical code component located on top of the MM first stage requiring code handler control when it is loaded with an operational L'-code. The CSD(M) provides continuity for the missile ignition safe/arm device for the first stage. A test coded CSD(M) is Unclassified and requires no special controls. **(T-0)**

6.9.5.1. Store an operationally coded CSD(M) that cannot be recoded in a split-handled container of the appropriate control group in the vault or SE. **(T-0)**

6.9.5.2. Decertify a CSD(M) when the operational L'-code is replaced with a non-operational code (maintenance). If the CSD(M) cannot be coded establish code handler (XX) control with the start of missile removal from the missile support ring. A code handler team (XX) will observe the removal of the CSD(M) at the MSB and will return the coded

CSD(M) to OSB. OSB will store the CSD(M) in a split-handled container of the appropriate control group in the vault or SE until supersession of the operational code. When the CSD(M) is returned to depot for repair, it is decertified and declassified when the appropriate team and repair facility technicians verify the code has been erased. **(T-0)**

6.9.6. The KS-60 contains the active and reserve keys necessary for encryption and decryption of message traffic between the LCC (HICS key) and LF (HICS key). Only CCSD-certified KS-60s listed on COMSEC account 613202 will be used in operational LFs. All KS-60s at the unit are Secret//CRYPTO//NOFORN and are controlled IAW EAP-STRAT Vol 16. An operationally keyed KS-60 is classified at the highest level of the keys, normally Top Secret//CRYPTO//NOFORN. OSB may direct battery removal of a keyed KS-60 for the specific purpose of dissipating electronic keys, but the KS-60 remains Secret//CRYPTO//NOFORN. **(T-0)**

6.9.6.1. **[377 TEG Only]**. LF KS-60s used at the 576 FLTS/DOX have been administratively decertified and designated "NON-TPC USE ONLY". Store Non-TPC and TPC KS-60s in separate locations. **(T-0)**

6.9.6.2. Visually inspect KS-60s for damage upon receipt and prior to dispatch and return from the field. The inspection will include exterior surfaces, pins, battery hinge, and battery holder for damage beyond normal wear and tear. Minor chips in paint are expected and acceptable.

6.9.6.3. Store damaged KS-60s in the vault until disposition and attach a DD Form 1577-2. Unit level maintenance beyond TO-authorized procedures is strictly prohibited. If damage occurs to a KS-60 or a KS-60 fails to load on the WCPS or accept a key in the field, send a SIPR email to USSTRATCOM/J374 identifying the KS-60, affected key registers, nature of damage or failure, circumstances, and any other pertinent information. An information copy will be sent to 20 AF/A3NB, AFGSC/A3ON and DIRNSA/C62. **(T-0)**

6.9.6.4. All OSB COMSEC SKLs used to insert a code or electronic key must be verified using WMAP Unload KS-60 Trace Data from SKL Procedure. This function allows the WCPS to receive trace data from a fielded KS-60 via an OSB COMSEC SKL connected to the WCPS. Trace data is the KS-60 status in response to a key load operation. Trace data must be retained with site installation paperwork. **(T-0)**

6.9.6.4.1. If damage occurs store damaged SKLs in the vault until disposition and attach a completed DD Form 1577-2 IAW T.O. 00-20-3. If damage occurs to a SKL or a SKLs to load on the WCPS or accept a key in the field, contact the base COMSEC custodian identifying the SKL, failure circumstances and any other pertinent information. Also inform USSTRATCOM/J374 via secure means of the issue in the form of a Codes Related Event. An information copy sent via secure means will be sent to 20 AF/A3NB, AFGSC/A3ON and DIRNSA/C62

6.9.7. The CSD(G) is not a critical component but must be verified on the WCPS and maintained under appropriate control from WCPS verification until LF removal and release from operational use by OSB. The CSD(G) control date will be the date OSB verifies the CSD(G) operation. **(T-0)**

6.9.7.1. After removal from an LF, the CSD(G) must be re-verified on the WCPS before being purged by E-Lab. If proper control is not lost, reverification is not required. Verification of a CSD(G) is required following E-Lab's checkout; E-Lab must purge the CSD(G) following the verification. **(T-0)**

6.9.8. A Coded MGS computer will be controlled with the appropriate team within the MGS vault. The control date is the date it arrives at OSB. **(T-0)**

6.9.8.1. Store operationally Coded MGS computers in split-handled containers of the appropriate control group in the MGS vault. **(T-0)**

6.9.8.2. Coded computers will be processed by an authorized TPC team from BGRC dispatched to the missile units. Code Controllers will escort BGRC team members while visiting OSB. Store the MGS in a split-handled container of the appropriate control group in the MGS vault until supersession of operational codes. After code supersession, AFGSC will direct disposition of the MGS. **(T-0)**

6.9.8.3. Coded MGCs are controlled IAW EAP-STRAT Vol 16 within the MGS vault. The control date is the date it arrives at the MGS vault. Store operationally launch-coded MGS computers in the MGS vault. **(T-0)**

6.9.8.3.1. **[377 TEG Only]**. A Coded MGS computer is classified Secret. Test launch coded MGS computers do not require any special controls. **(T-0)**

6.9.8.4. Launch-coded computers will be processed by an authorized TPC team from BGRC dispatched to the missile units. Code controllers will escort BGRC team members while visiting OSB. The BGRC team will remove the magnetic memory unit from the MGC and mark it with the classification level, the MGS number the unit was removed from, attach serviceability tags and give the magnetic memory unit to the code controllers. Code Controllers will store the magnetic memory unit in the SE until supersession of operational code. After code supersession AFGSC will direct disposition of the magnetic memory unit. The remainder of the MGC, without the magnetic memory unit, can be shipped to BGRC for repair via an approved carrier. **(T-0)**

6.9.8.5. **[377 TEG Only]**. An LFLCD-coded MGS computer is classified Secret. Test LFLCD and Pen-Coded MGS computer do not require any special controls. **(T-0)**

6.10. LCC Components (All TDI references do not apply to the 576 FLTS).

6.10.1. An LCP becomes a critical component at the beginning of its coding on the WCPS. Its control date is the date of coding on the WCPS. MCUs A/B form the complete launch code (MCU B also contains an LCC identifier) and MCU C contains the inhibit code. In the vault, control all LCPs IAW EAP-STRAT Vol 16. Test coded LCPs are Unclassified but require two officer control. Store LCPs in open storage in the SE. **(T-0)**

6.10.1.1. Launch switches will be verified and sealed with a TDI by code controllers before panels are issued for field use. The classification and LCC assignment will be clearly marked on each panel. **(T-0)**

6.10.1.2. An LCP may be administratively decertified whenever all the operational codes processed by the panel are superseded. **(T-0)**

6.10.1.3. LCP keys are Unclassified and are controlled IAW EAP-STRAT Vol 16. This control requirement begins at the start of key switch verification and ends when the LCP is removed from the LCC unless the same panel is to be reinstalled in the LCC without being recoded (e.g., Rivet MILE, SELM, etc.). Store launch keys in open storage in the vault. **(T-0)**

6.10.1.3.1. **[377 TEG Only]**. Launch keys will not be issued to FDE task force personnel. Keys will be issued to 576 FLTS/ personnel who will release keys to task force as required. **(T-0)**

6.10.1.4. Code controllers will verify LCP keys by inserting each key (primary and duplicate) in the LCP switch and rotating the keys to ensure both keys and switch work properly. An original and duplicate copy of the LCC Launch Key Verification Record will be completed. Both copies (original and duplicate) of the Launch Key Verification Record will be signed by the two code controllers who accomplished the verification action. The original Launch Key Verification Record will be laminated and attached to the primary key by code controllers, so it does not interfere with key switch operation when the key is inserted. The duplicate Launch Key Verification Record will be laminated and attached to the duplicate key maintained in OSB. The LCC Launch Key Verification Record will be used by the MCC to verify launch keys match launch switches. The LCC Launch Key Verification Record is attached to the LCP. **(T-0)**

6.10.2. The LEP becomes a critical component at the beginning of its coding on the WCPS. Its control date is the date of coding on the WCPS. In OSB, control all LEPs IAW EAP-STRAT Vol 16. Store LEPs in the appropriately controlled container in the vault, secure area, or SE. Clearly mark the classification and LCC assignment on each panel. An LEP may be administratively decertified when all the operational codes processed by the panel are superseded. **(T-0)**

6.10.2.1. **[377 TEG Only]**. Test coded LEPs are Unclassified and controlled IAW EAP-STRAT Vol 16. **(T-0)**

6.10.3. The KS-60 contains the active and reserve keys necessary for encryption and decryption of message traffic between the LCC and LF. Only CCSD-certified KS-60s listed on COMSEC account 613202 will be used in operational LCCs. All KS-60s at the unit are Secret//CRYPTO//NOFORN and require control IAW EAP-STRAT Vol 16. An operationally keyed KS-60 is classified at the highest level of the keys, normally Top Secret//CRYPTO//NOFORN and will be controlled IAW EAP-STRAT Vol 16. OSB may direct battery removal of a keyed KS-60 for the specific purpose of dissipating electronic keys, but the KS-60 remains Secret//CRYPTO//NOFORN. **(T-0)**

6.10.3.1. Visually inspect KS-60s for damage upon receipt and prior to dispatch and return from the field. The inspection will include exterior surfaces, pins, battery hinge, and battery holder for damage beyond normal wear and tear. Minor chips in paint are expected and acceptable. **(T-0)**

6.10.3.2. Document equipment failures or discrepancies of USSTRATCOM/J374-owned equipment/COMSEC items (i.e., KS-60) IAW T.O 00-20-3 and by memorandum or email to USSTRATCOM/J374, with a courtesy copy to 20 AF/A3NB, AFGSC/A3ON and

DIRNSA/C62 for corrective action. The appropriate tags must be affixed to each equipment item reflecting the specific issue. **(T-0)**

6.10.3.3. All OSB COMSEC SKLs used to insert a code or key must be verified using WMAP unload KS-60 trace data from SKL procedure. This function allows the WCPS to receive trace data from a fielded KS-60 via an OSB COMSEC SKL connected to the WCPS. Trace data is the KS-60 status in response to a key load operation. Trace data must be retained with site installation paperwork. Store damaged SKLs in the vault until disposition and attach a completed DD Form 1577-2 IAW T.O. 00-20-3. If damage occurs to an SKL or SKLs fails to load on the WCPS or accept a key in the field, contact the Base COMSEC custodian identifying the SKL, failure circumstances and any other pertinent information. Also contact USSTRATCOM/J374 via secure means with the same information in the form of a Codes Related Event. An information copy also via secure means will be sent to 20 AF/A3NB, AFGSC/A3ON and DIRNSA/C62. **(T-0)**

6.10.4. The WSP becomes a critical component at the beginning of its OPCERT procedure until decertification. The control of the WSP and its subcomponents depends on code exposure. See EAP-STRAT Vol 16 for potential code exposure. **(T-0)**

6.10.4.1. Store failed translate-coded, launch-coded and J-coded WSPs in OSB under proper controls until all affected codes are superseded. **(T-0)**

6.10.4.2. A WSP loaded with C(a)C(b) control words is classified Secret//CRYPTO and controlled IAW EAP-STRAT Vol 16 until squadron BS/L keys in all squadron LCCs are changed or until decertification. Ensure HDAs are reloaded with new I-codes to reflect change out of new BS/L keys. **(T-0)**

6.10.4.3. The WSP and its subcomponents can be administratively decertified when the codes exposed to the WSP are superseded. **(T-0)**

6.10.5. The HDA is contained within the BS/L to provide storage of all programs and data. I Codes on the HDA are encrypted; therefore, the HDA is not a code component but will be controlled based on its highest classification. A TS-loaded HDA will be controlled with two properly cleared couriers when transporting to and from the LCC per DoW Directive S-5210.81. A Secret loaded HDA only requires one properly cleared courier. Once loaded, the HDA remains classified at the highest level of the data it ever contained until it is destroyed. **(T-0)**

6.10.5.1. The HDA may be overwritten by depressing the overwrite key on the OID, which commands the Console Operating Program (COP) to perform an overwrite but will not declassify the HDA. If the COP does not indicate a successful overwrite or if overwrite cannot be initiated, the HDA can be returned to OSB and initialized on the WCPS. If the HDA initialization is successful, the HDA can be loaded with data and returned to operational use in an LCC. Control the HDA as a classified component based on the classification level of the data it contains until it can be declassified by removing the disks or HDA flash memory card. The HDA casing can be turned in through supply channels. **(T-0)**

6.10.5.2. Disposition of the HDA memory depends on the design of the particular HDA. The older design uses disk memory while the newer design uses solid-state flash memory. Reference T.O. 31X8-2-2-1 to remove classified HDA disks. This procedure will be used

only on defective HDAs. Destroy HDA disks by removing the entire recording surface of the disk by either sanding or grinding using an emery wheel or sander, sandblasting, or bead blasting. **(T-0)**

6.10.5.3. HDA solid-state memory failure requires removal of flash memory card IAW T.O. 31X8-2-2-1 procedures. Properly mark the memory card with the classification and attach serviceability tags. Store the flash memory card in the vault or SE until transfer to AFGSC. AFGSC will deliver failed flash memory cards to DIRNSA/C62 for destruction. **(T-0)**

6.11. OLYMPIC STEP.

6.11.1. Wing OSBs will participate in all planning activities for the operation. The following actions must occur prior to building code materials for the operation. These steps do not apply to 576 FLTS/DOX.

6.11.1.1. A/B Media. Coordinate to receive new WCPS A/B media, ITKs, and TVs from USSTRATCOM/J374 before the planned start date of the annual squadron code change. A storage key will be selected and provided on a WCPS Key CD Pair.

6.11.1.2. TEKs Selection. New TEKs (BS/L, HICS keys, and REKs) will be selected from Wing Pool key CDs for each squadron.

6.12. Coding Operations.

6.12.1. All WCPS operational and test coding not requiring split-knowledge will be performed by a team of certified code controllers who meet both two officer and AB requirements. **(T-0)**

6.12.1.1. **[377 TEG Only]**. Coding may be performed by a team of any certified code controllers. Split handling/knowledge operations will be performed by a team of certified code controllers who meet either officer or enlisted and AB requirements. **(T-0)**

6.12.2. The SCC will make the final determination as to who can view operational WCPS coding. IAW AFI 91-114, personnel cannot have unescorted access (to include accompanied alert duty) to an LF or LCC if they have had access to operational coding operations (e.g., cannot be part of a TPC team at the LF or LCC). The following personnel (except Combat Mission Ready qualified personnel) are eligible to view operational WCPS coding if approved by the SCC: wing commander, vice wing commander, group commanders, deputy group commanders, missile squadron commanders and operations officers, missile maintenance squadron commanders, USSTRATCOM/J374 personnel, AFGSC/A3ON personnel, 20 AF/A3NB personnel, HQ AFGSC Inspector General inspectors and certified code controllers and selectees. Code controller selectees must have documentation assigning them to OSB prior to WCPS training and are prohibited from handling operational components.

6.12.3. No electronic equipment, other than required for coding support, may be inside the SE during operational coding. When operational or test codes are being loaded or processed, the SE door must be closed and sealed under pneumatic pressure. If entry or exit is required during these operations, the console must be in the “menu display” mode before opening the SE door. PVS key loading operations will only be conducted with the SE door fully closed and sealed with a minimum of two officer AA or BB code controller team in the SE. Ensure a split-knowledge control team meets all requirements for components present during split-knowledge operations. Procedures involving only the PVS key and SYSTEM disk (e.g.,

System Boot-Up, Self-Tests and Certification Tests) are not considered operational coding and may be performed with the SE door open, once the split-knowledge PVS key load is accomplished. **(T-0)**

6.12.3.1. **[377 TEG Only]**. PVS key loading operations will only be conducted with the SE door fully closed and sealed and any AB code controller team in the SE. **(T-0)**

6.12.4. Once used to process operational or test code material, the Hewlett-Packard 1000 computer is classified Top Secret and must be controlled by the appropriate code controllers. Other WCPS console drawers or components in the “red sensitive” area (Bays 5 and 6, Cathode Ray Tube (CRT) and Keyboard) are classified Top Secret and must remain in the vault under control IAW EAP-STRAT Vol 16. Some components may require additional controls based on code exposure as defined in this publication. These devices may be declassified and leave the vault only if all memory retention subassemblies are removed (X-ray other parts to verify only authorized memory modules exist) or when all codes processed by the equipment have been superseded. Since no approved overwrite procedures exist, requests for waivers must be submitted to DIRNSA/C62 and USSTRATCOM/J374 via 20 AF/A3NB and AFGSC/A3ON. **(T-0)**

6.12.5. The PROM Fuser Verifier and tapes are critical components and will be stored in the vault or SE under TPC control. **(T-0)**

6.12.6. If a unit OSB/576 FLTS/DOX encounters a problem with the WCPS and coding capability is lost, notify USSTRATCOM/J374 and 20 AF/A3NB who will keep AFGSC/A3ON apprised of the situation.

6.12.6.1. If E-Lab troubleshooting fails to resolve a problem, the OSS/CC or 576 FLTS/CC will forward a request for Contractor Logistical Support (CLS) on-site support through 20 AF/A3NB to ICBMSD. Coordination copies will be sent to AFGSC/A3ON and USSTRATCOM/J374.

6.12.6.2. Ensure readiness reporting is accomplished through DRRS as required. Recovery and follow-on actions will be a coordinated multi-agency effort.

6.12.6.3. Retain any failed WCPS circuit cards or other electronic WCPS components, both Type 1 and Type 2, awaiting destruction under code control until decertified or requested by USSTRATCOM/J374. Decertified circuit cards that have processed code or encrypted data remain classified CRYPTO items. USSTRATCOM/J374 will either deliver failed components to DIRNSA/C62 for destruction or provide instructions for removal of specific CRYPTO components for return to DIRNSA/C62 and destruction of the remaining circuit cards. **(T-0)**

6.12.6.4. Decertification requirements are outlined in T.O. 31X8-2-2-2 or T.O. 21M-LGM30F-12-1. Contact USSTRATCOM/J374 via 20 AF/A3NB for guidance on interim storage and control of all electronic components requiring destruction. Dispose of decertified materials per USSTRATCOM/J374 instructions. **(T-0)**

6.12.7. PVS Master Key CDs and PVS Key Load Verification sheets will be controlled and stored split-knowledge components. All media encrypted using the KS-60 will be controlled IAW EAP-STRAT Vol 16 and stored in the SE. **(T-0)**

6.12.7.1. KEKI CDs. At the wing, the KEKI CD pair is read, and each key dataset is saved on the WMAP data disk assigned to the appropriate LCC or LF. When an External KS-60 is loaded at the WCPS for an ICU II configured site, the KEKIs assigned to the site are loaded into the KS-60's KEK registers. KEKI-A and KEKI-B CDs must be destroyed after being successfully loaded onto a data disk, KEKI files purged from the recordkeeping disk and appropriate destruction forms verified by USSTRATCOM/J374 before the associated TV/ITKs may be received by the wing.

6.12.7.2. TV and ITK CDs. USSTRATCOM will send the IT Keys after confirmation of the destruction of the KEKI CDs in the form of an AF 153 sent via secure means to J374. Irreversibly transformed code data and variable data are generated at USSTRATCOM and written to a TV CD. A TV CD supports from one to all 50 LFs in a squadron as selected by the operator. Concurrently, an ITK CD is generated. The TV CD and ITK CD are sent to the wing. The TV CD may support operational or test code usage; this operator selection is reflected on the TV CD label but does not otherwise affect the TV CD contents.

6.12.7.3. Complementary PVS and data encryption materials will not be out of their containers at the same time except when installing them in the WCPS console. When properly installed in the WCPS, the PVS keys, PVS encrypted SYSTEM disk and the encrypted DATA disk are considered an integral part of the WCPS which is therefore controlled by a code controller team. PVS Key CDs of the opposite control group will not be out of their containers at the same time. PVS loading operations are strictly split-knowledge operations. Retain superseded and failed PVS and data encryption material until destruction is authorized by USSTRATCOM/J374. Mark all materials awaiting destruction. **(T-0)**

6.12.8. OSB/576 FLTS/DOX receive WCPS Key CDs and Wing Pool CDs from USSTRATCOM/J374 on an annual basis or as needed to support contingency situations. OSBs also receive a PVS Key CD set. Each CD set has a Group A and a matching Group B CD with the following number of keys: WCPS Key CD – One Storage Key and/or one Media Key and one Link Key. Wing Pool CD – Total number of encryption keys dependent on wing: Wing 1, Wing 3 and Wing 5 (8,000) and Wing 7 (1,000). PVS Key CD – 100 TEKs. Upon receipt of new Wing Pool Key CD set, OSBs will load within 10 duty days and will notify USSTRATCOM/J374 when complete. Control superseded or failed PVS and data encryption material IAW EAP-STRAT Vol 16.

6.12.8.1. Store damaged Key CDs in the vault in the appropriately controlled storage containers until disposition is directed from USSTRATCOM/J374. When damage occurs to a Key CD or a Key CD fails to read on the WCPS (or DMD for PVS Key CDs), send a SIPR email identifying the Key CD, affected key registers, nature of damage or failure, related circumstances, and any other pertinent information to USSTRATCOM/J374 via 20AF/A3NB and AFGSC/A3ON, with an information copy to DIRNSA/C62. **(T-0)**

6.12.8.2. Retain superseded and failed Key CDs until destruction is authorized by USSTRATCOM/J374. Mark all Key CDs awaiting destruction. Destruction at OSB will be accomplished by NSA-approved CD shredding or disintegration technology only. **(T-0)**

6.12.9. WCPS KS-60s provide the encryption necessary for the operation of the WCPS. The WCPS uses two KS-60s (PVS and SYSTEM) which are classified Secret//CRYPTO//NOFORN and controlled IAW EAP-STRAT Vol 16. Once loaded with

operational keys the KS-60 takes on the highest classification of the keys loaded and typically are Top Secret//CRYPTO//NOFORN items. **(T-0)**

6.12.9.1. Store damaged KS-60s in the vault until disposition is directed from USSTRATCOM/J374 and attach a completed DD Form 1577-2 IAW T.O 00-20-3. Unit level maintenance beyond TO-authorized procedures are strictly prohibited. If damage occurs to a KS-60 or a KS-60 fails to load on the WCPS or accept a key in the field, send a SIPR email to USSTRATCOM/J374 identifying the KS-60, affected key registers, nature of damage or failure, circumstances, and any other pertinent information. An information copy will be sent to 20 AF/A3NB, AFGSC/A3ON and DIRNSA/C62. **(T-0)**

6.12.10. WCPS magneto-optical system disks are Unclassified components because they are encrypted with the PVS key controlled IAW EAP-STRAT Vol 16 and may be stored in open storage in the SE. Their control date is the date of creation on the WCPS. OSB will maintain at least one backup SYSTEM disk. Failed SYSTEM disks remain under appropriate control in the SE until they are destroyed. **(T-0)**

6.12.10.1. WCPS DATA disks include wing code disks, backup disks, recordkeeping disks and certification disks. WCPS DATA disks are controlled IAW EAP-STRAT Vol 16. **(T-0)**

6.12.10.1.1. Wing code and backup disks are classified according to the highest classification of support data (not code data) stored on the disk. Operations disks will normally be classified Top Secret//FRD due to the highest classification of the support programs loaded on the disk. They retain their classification until they are destroyed or degaussed. **(T-0)**

6.12.10.1.2. Backup Disks. OSB will maintain a minimum of two DATA disk backup copies of the operational wing code DATA disk. 576 FLTS/DOX will maintain a minimum of two DATA disk backup copies of the test wing code DATA disk. Update these backup disks anytime an operational P-Plug is loaded. Operational P-Plugs will not be issued to the field unless they are on two backup disks. Unless no coding activity has occurred, OSB will update the backup disks at least weekly to avoid loss of coding records. **(T-0)**

6.12.10.1.3. Recordkeeping DATA Disks. A recordkeeping DATA disk is controlled IAW EAP-STRAT Vol 16 when it has been used to receive or transfer code data via the link. Disks remain that control until the disks are destroyed. **(T-0)**

6.12.10.1.4. Certification Disks. Certification DATA disks which have never been exposed to operational codes are not code components.

6.12.10.2. Destruction. Magneto-optical disks that have seen encrypted data or classified support data must be destroyed by either burning or pulverizing. When material is pulverized all residue must be reduced to pieces sized 0.25 millimeters or smaller. Residue destroyed by burning must be reduced to white ash. **(T-0)**

6.12.10.3. Failed Disk Drive. Control failed disk drives having seen operational codes appropriately until all PVS keys and Worldwide Unlocks used on it are superseded and returned to USSTRATCOM/J374 or the disk is destroyed. Failed disk drives are CRYPTO until destroyed. **(T-0)**

6.12.11. MCU Encoder Drawers. These drawers are always critical components and become code components after being used to code MCUs. Store uninstalled drawers in the SE under the appropriate control until the codes processed by the drawer have been superseded. Mark all MCU Encoder Drawers with a tag or label denoting date of latest code exposure and squadrons affected. Do not return failed MCU Encoder Drawers or those requiring refurbishment through supply channels until after codes supersession or upon successful completion of an MCU Certification Test on the WCPS. Between 1 November and 15 January units will test all MCU Encoder Drawers. Verify three MCUs can be properly coded using all patterns in the MCU Certification Test. **(T-0)**

6.12.12. MCUs. The MCU assumes critical component status upon successful completion of the WCPS functional check of the MCU. Once coded, the MCU remains a code component until decertified. An MCU that cannot be dissipated must be marked and properly controlled until the last verified code (the launch, inhibit, or J Code) it was coded with is superseded. MCUs may be decertified by either method listed below. **(T-0)**

6.12.12.1. Code Supersession. MCUs may be administratively decertified after launch or J code supersession. **(T-0)**

6.12.12.2. Test MCUs by encoding with all of the WCPS certification test patterns. The MCU is decertified after the correctness of the code has been verified. **(T-0)**

6.12.13. Master Code Media. All master code media will be stored in the SE and will not be removed except for destruction or disposition purposes. If damage to the media is suspected, two officer code controllers of the proper control group may examine, to the minimum extent necessary, the suspected part of the media. If damage occurred, the media will be conspicuously marked and replaced with a spare. Report cases of master media damage to USSTRATCOM/J374 not later than the first duty day following discovery of the damage. **(T-0)**

6.12.13.1. Master A and Master B Media. Master A and Master B media are controlled and stored IAW EAP-STRAT Vol 16. A/B media are both encrypted using the unit's WCPS Storage Key. OSB will request permission from USSTRATCOM/J374 to destroy all Master A/B media encrypted in the old key. After supersession of the Storage key, document destruction on AF Form 310. Send one copy to USSTRATCOM/J374 for UMR update. **(T-0)**

6.12.13.2. Master P Media. PEN blocks on Master P media are loaded into the WCPS to assign PEN codes to LFLCDs. Master P Code media may be stored in either Group A or Group B storage containers or in open storage within the SE. **(T-0)**

6.12.13.2.1. OSB Operations. Always perform the exclusions test when loading PEN data into the WCPS. PEN code blocks are one time use code data. Operational blocks of PEN code data used to compute a CMSC will not be reused. OSB will not simultaneously issue components containing complementary PEN C and PEN D Data (from the same file and block). This does not apply to the 576 FLTS/DOX. **(T-0)**

6.12.13.2.2. PEN Data Supersession. Penetration codes are superseded when OSB declares them superseded. Physical destruction of the affected code is not required; however, positive measures and actions must be taken to ensure superseded codes are not inadvertently reused. **(T-0)**

6.12.13.2.3. Disposition. Return media to USSTRATCOM/J374 or destroy by disintegration technologies when directed by USSTRATCOM/J374. Document disposition on SF 153. **(T-0)**

6.12.13.3. Master I Media. I Codes are loaded from Master I media into the WCPS to produce 32-bit C(a) and C(b) control words used for calculating CMSC values for LFLCDs, HDAs and incremental floppy/flash disk uploads. Master I Code media may be stored in either the appropriate controlled storage containers or in open storage within the SE. **(T-0)**

6.12.13.3.1. OSB/576 FLTS/DOX Operations. Once loaded at an LF or LCC, blocks of I Code data will not be reused in the field. When replenishing I Codes with a new edition, OSB/576 FLTS/DOX will ensure any remaining I Code blocks from the previous edition are superseded. **(T-0)**

6.12.13.3.2. Disposition. Return media to USSTRATCOM/J374 or destroy by disintegration technologies when directed by USSTRATCOM/J374. Document disposition on SF 153. **(T-0)**

6.12.13.4. Master N Media. Master N media contain P-Plug data maintained at OSB/576 FLTS DOX. Store Master N media in appropriate split-handled containers within the SE. Store Master N media awaiting destruction separate and in a different location than Master N media still in use or held in reserve. **(T-0)**

6.12.13.4.1. OSB/576 FLTS Operations. P-Plugs will be verified against their Master N media before going to the field. Exceptions must be approved by OSB/576 FLTS. **(T-0)**

6.12.13.4.2. Disposition. Once all P-Plugs on a Master N media are awaiting destruction or destroyed return media to USSTRATCOM/J374 or destroy by disintegrating when directed by USSTRATCOM/J374. Document disposition on SF 153. **(T-0)**

6.12.14. DMD. The DMD is a laptop computer used to load PVS keys to the WCPS.

6.12.14.1. OSB/576 FLTS/DOX Operations. Laptops become DMDs and require TPC once loaded with the DMD software. DMDs at OSB become Top Secret//CRYPTO//NOFORN with split-knowledge control once loaded with a PVS Key CD, and Secret//CRYPTO//NOFORN at the 576 FLTS/DOX. Proper OSB/576 FLTS/DOX teams should turn on the laptops and charge the batteries at least once per month to verify operation and extend the life of the equipment to maximum extent possible. An ideal time to accomplish this action is during the 30-day inventory when the DMDs are inventoried. Ensure this action is logged in the coding shift log. **(T-0)**

6.12.14.2. Damage. Failed DMDs maintain their classification and control. Store damaged DMDs in the OSB/576 FLTS/DOX vault in applicable appropriately controlled storage containers until disposition is directed from USSTRATCOM/J374. When damage occurs to a DMD or a DMD component fails, a Secret message identifying the DMD, nature of damage or failure, related circumstances and any other pertinent information will be sent to USSTRATCOM/J374 with info copy to DIRNSA/C62, 20 AF/A3NB, and

AFGSC/A3ON. The spare DMD will then be used to replace the damaged or failed DMD and will be controlled appropriately. **(T-0)**

6.12.14.3. Disposition. Failed DMDs require destruction by DIRNSA/C62. OSB will retain damaged/failed DMDs until AFGSC/A3O in coordination with USSTRATCOM/J374 directs actions for removal and replacement. **(T-0)**

6.12.15. OSB COMSEC SKL. OSB COMSEC SKLs are unclassified COMSEC controlled items which will be used by an XX team. System design requires OSB/576 FLTS/DOX personnel be designated as SKL SSOs in order for the WCPS to perform audit data functions. When a COMSEC SKL is used, perform unload KS-60 Trace Data as required. Performing an SKL Audit Function is not required but may be performed to aid in troubleshooting or when directed. Store SKLs in the vault until disposition is directed from the Base COMSEC custodian and attach a completed DD Form 1577-2 IAW T.O 00-20-3. **(T-0)**

6.13. WCPS Maintenance Requirements. Maintain the WCPS IAW applicable technical orders (T.O. 31X8-2-2-2 and T.O. 31X8-2-3-1). To the maximum extent possible, WCPS maintenance functions are performed outside the SE using the HCVE. Personnel maintaining the WCPS must be certified under PRP and qualified to perform maintenance on the WCPS. Depot assistance will be obtained through 20 AF/A3NB to accomplish major maintenance or extensive Time Compliance Technical Order (TCTOs) if support equipment or required skills are not locally available. Notify USSTRATCOM/J374 of a WCPS outage per the EAP-STRAT Vol 16. Notify 20 AF/A3NB if unable to conduct coding operations for a period exceeding 24 hours. ELAB is the primary contact to conduct WCPS repairs. If ELAB is unable to complete repairs, they may contact the Boeing hotline for assistance. If the hotline is unable to provide resolution, contact 20 AF/A3NB to coordinate on-site contractor support. An anomaly log will be maintained containing all WCPS coding anomalies. A copy of this log will be sent to 20 AF/A3NB and AFNWC/NIAG monthly. Faults caused by code controller error do not require reporting.

6.14. Hardware Certification and Verification Equipment (HCVE). The HCVE bench is part of the nuclear certified WCPS and is a critical component. It permits WCPS hardware troubleshooting, diagnosis, and repair within the TPC-controlled vault environment. The HCVE is maintained inside a TPC-controlled vault. **(T-0)**

Chapter 7

WEAPON SYSTEM TESTING

7.1. General. Code components, programs, and miscellaneous materials required for training, testing, or other non-operational purposes are issued by OSB/576 FLTS/DOX. Code components used for these purposes will be test, test designated, or training components.

7.1.1. Test Codes and test code components are used to satisfy training, test, and other non-operational coding requirements, such as WCPS coding demonstrations and WCPS code controller evaluations and training sessions. Other miscellaneous material and programs required for these purposes may be operational if test or training versions have not been provided. Notify 20 AF/A3NB of these instances.

7.1.2. Test code components are controlled the same as operational components when they are used to train code handling procedures, to demonstrate code handling proficiency, or to satisfy a test objective of operational realism.

7.1.3. Components used to satisfy test or training requirements are labeled to distinguish them from operational components. Labels will indicate component type, classification, and purpose. For example, Test LFLCD (S), IG/20 AF OBS, or Test LFLCD (U) TNG PURPOSES, or Test CCV (U) TNG PURPOSES.

7.1.4. The unit training LF(s) will be configured with a test P-Plug, test codes selected from the Test Master Data, and an operationally keyed KS-60. The CSD(M) may be either operationally or test coded, but the missile safing pins may not be removed unless the CSD(M) is operationally coded, or the MGS is shut down for the duration of the missile safing pins removal. **(T-0)**

7.1.4.1. Due to the operational flight program re-entry vehicle mismatch function, a re-entry system simulator can only be configured a limited number of ways. To ensure MOSR 38, SBNG does not occur upon startup of the training LFs, the unit OSB will coordinate with OSX and maintenance personnel to ensure the configuration is loaded as requested.

7.1.5. Items designated for training will be marked "TRAINING AID." These items are Unclassified and do not require special handling.

7.1.6. If a furnished test component is damaged, send a request for a replacement to the appropriate agency through 20 AF/A3NB. Destroy the damaged component after its replacement arrives.

7.2. Simulated Electronic Launch Minuteman (SELM) (GIANT PACE) (This does not apply to the 377 TEG).

7.2.1. SELM test coding activities will be accomplished IAW AFI 91-114, this publication and other applicable directives. Operational code controls apply for SELM test except as noted in AFI 91-114 and in the following paragraphs. **(T-0)**

7.2.2. Operational MGSs selected for SELM will be overwritten before SELM posturing. SELM-coded MGSs will be overwritten prior to reposture to operational status with an LFLCD load followed by an RDCC. **(T-0)**

7.2.3. A test P-Plug will be used for SELM activities. A SELM P-Plug removed from a failed SELM MGS may be installed in the new SELM MGS. During operational reposture, the SELM P-Plug will be replaced with a new operational P-Plug. **(T-0)**

7.2.4. Equipment containing only SELM codes may be released to contractor personnel for failure analysis if required. Control requirements for these situations will be provided by USSTRATCOM/J374 and 20 AF/A3NB. **(T-0)**

7.2.5. SELM coding activities will be accomplished using test P-Plugs and excluded test master data (X, Y, L, and L') for LFs and test LCCs. Test PEN and I Code data for SELM will be selected from the test master data located at each OSB. Excluded test A/B media and KEKI, ITK, KEKT, REK, and TV media will be provided by USSTRATCOM/J374. Use operationally keyed KS-60s but with a test ITK and load the HDA with operational I Codes for SELM. **(T-0)**

7.2.6. OSB Operations. The SELM DATA disk will contain master code data and LF support data. OSB will maintain at least one backup SELM DATA disk. OSB will create LFLCDs and encode CCVs, LCPs, DTUs, LEPs, LF KS-60s, LCC KS-60s, RDCK RSM, and RDCC RSM as required. CSD(G) replacement may be required for reposture. **(T-0)**

7.2.6.1. OSB will coordinate with OSX and the 377 TEG to ensure the LF configuration is specified on the Test Execution Instruction (TEI). Reference [paragraph 7.1.4.1](#).

7.2.7. Holographic TDI Sealing. SELM LCPs (panels and switches) and SELM LEPs will be sealed with operational holographic TDIs. Two awake MCCMs will control the LCP IAW EAP-STRAT Vol 16 while the key switch seal is off. This applies from the time of operational holographic TDI removal for SELM key turn until the keys are locked in the panels due to SELM key turn. **(T-0)**

7.3. Hardness Surveillance Electromagnetic Pulse (EMP) Program (HSEP) (This does not apply to the 377 TEG).

7.3.1. Test Materials. The intent of HSEP is to determine the current EMP hardness level of the Minuteman weapon system and to project hardness degradations to allow for corrective action by the ICBM Systems Directorate.

7.3.2. HSEP coding activities will be accomplished using HSEP Test Master Data (X, Y, L, and L') for LFs. USSTRATCOM/J374 will provide HSEP A/B media as well as KEKI, ITK, and TV media for ICU II complete sites to the unit for coding via transmit data via link. Annually, the Boeing Company codes lab will provide HSEP with a 100 key subset of the contractor A/B Master key CD pair specifically created for this purpose. This CD pair is classified Secret//CRYPTO//NOFORN. The pool CD pair will be loaded to the HSEP DMD. The DMD will also be classified Secret//CRYPTO//NOFORN. Unit OSBs may store the laptop and key CD pair but they must be stored separately from operational keys. These items may be transported from unit to unit by DCS courier or a courier team designated by the controlling authority (USSTRATCOM/J374). HSEP will also maintain two Secret//CRYPTO//NOFORN HDAs coded with a contractor BS/L key. The HDAs will be coded annually using new key CD pairs provided by Boeing. This will normally occur when HSEP relocates from one unit to another. **(T-0)**

7.3.3. General Dynamics will provide a DISS visit request for the duration of the test to the affected unit's Security Management Office (SMO) 30 days prior to arrival so the unit can verify clearance information. OSB may then allow HSEP personnel to enter the codes area. HSEP personnel will sign in on the visitor log and be escorted.

7.3.4. General Dynamics will provide SD Form 572, *Cryptographic Access Certificate (PA) (CUI)*, for each contractor or memorandum to the affected unit OSB 30 days prior to arrival. The unit will verify contractors have a minimum Secret clearance and meet required COMSEC training requirements prior to transferring any COMSEC items to the HSEP team.

7.3.5. The MGS, P-Plug, and CSD(G) will be removed, the maintenance code inserted into the CSD(M), and the KS-60 zeroized prior to site turnover. The CSD(M) will be coded with an HSEP L' Code using the SMIC provided CCV. Proper control of the LF must be maintained at all times during the HSEP test period.

7.3.6. The LCP, LEP, and HDA will be removed from the LCC prior to HSEP turnover. The LCP and LEP do not need to be dissipated; they can be returned to OSB to be reinstalled after the HSEP is complete. Operational keys installed in the LCC KS-60 must be dissipated. Proper control of the LCC must be maintained at all times during the HSEP test period. The LCC selected for HSEP must be placed on superseded codes and keys.

7.3.7. OSB will transfer the LF or LCC KS-60 and one KS-60 from shelf spares to be used in the SDS to the General Dynamics COMSEC account for the duration of the test. Two authorized HSEP personnel will sign the SF 153 accepting the KS-60. The SF 153 transfer of the KS-60 to HSEP personnel may be processed by a qualified maintenance team during site turnover or may be accomplished by OSB at the codes vault. A KS-60 used during HSEP operations will be controlled by a proper handling team when outside of the codes vault. HSEP personnel may also request to store their HSEP CCV within the OSB vault during the buy and sell periods for LFs. Ensure the HSEP CCV is properly labeled and separated from operational CCVs. If any problems occur with the KS-60, HSEP personnel will immediately report the problem to OSB. If a KS-60 fails, OSB will send a SIPR email to USSTRATCOM/J374 identifying the KS-60, affected key registers, nature of damage or failure, circumstances, and any other pertinent information. An information copy will be sent to 20 AF/A3NB, AFGSC/A3ON and DIRNSA/C62. OSB may provide a replacement KS-60 from the spares inventory to HSEP personnel after ensuring enough spares are available to meet operational priorities.

7.3.8. LF Reposture. Install operational MGS, CSD(G), and operationally keyed KS-60. Install a new P-Plug. Place an operational L' in the CSD(M) and perform a Complete Load LFLCD load for the MGS and RDCK and RDCC. The KS-60 used during HSEP testing may be returned to operational use as long as proper control of the site has not been lost during the test period and no KS-60 anomalies occurred. If proper control of the site was lost at any point or an abnormal KS-60 indication was received, the KS-60 must be returned to CCSD for a new operational certification via a USSTRATCOM/J374 courier team. The contractor keys will be dissipated from the KS-60s used in the message processor, 403A4 drawer, and SDS before being returned to the codes vault. All power (including the battery pack) must be removed from the KS-60. The dissipated KS-60s used during HSEP operations will be controlled by a proper handling team when outside the codes vault.

7.3.9. LCC Reposture. Install operational LCP, LEP, and an operationally keyed KS-60. Encode and install a new operational HDA. The KS-60 used during HSEP testing may be returned to operational use as long as proper control of the site has not been lost during the test period and no KS-60 anomalies occurred. If proper control of the site was lost at any point or an abnormal KS-60 indication was received, the KS-60 must be returned to CCSD for a new operational certification via a USSTRATCOM/J374 courier team. The contractor keys will be dissipated from the KS-60s used in the CDA and SDS before being returned to the codes vault. The dissipated KS-60s used during HSEP operations will be controlled by a proper handling team when outside the codes vault.

Chapter 8

LATERAL CODING

8.1. General. When efforts to correct a WCPS outage are unsuccessful and the outage affects the unit's ICBM alert status, the SCC/FC will initiate lateral coding actions at another unit.

8.1.1. The requesting unit will submit, via SIPR email, a lateral coding request to 20 AF/A3 for coordination with AFGSC/A3O and USSTRATCOM/J374. Prior to making this request, the requesting unit will ensure all WCPS repair efforts are exhausted, including contractor assistance, before making the final request. Final approval for lateral coding will rest with 20 AF/CC with concurrence from USSTRATCOM/J37. Prior to final approvals, a complete lateral coding and relocation plan must be available for review. **(T-0)**

8.1.2. The requesting unit will confirm, and 20 AF will verify before authorizing, the lateral coding location can support all storage and handling requirements for required code materials while verifying separation from host unit code material.

8.1.3. OSB/576 FLTS/DOX will only transport code components in government vehicles or military aircraft.

8.1.4. Coding operations will be accomplished by the visiting code controllers, however two code controllers from the host OSB must be present during coding operations.

Chapter 9

REPORTING

9.1. General. This chapter provides guidance for reporting incidents involving ICBM keys or codes. Units must reference this document and the EAP-STRAT Vol 16 to properly report incidents. Following proper code handling and accounting procedures ensures the integrity of the ICBM codes system is maintained. Personnel involved in the control and handling of ICBM keys or codes must understand how to detect and report unauthorized or unusual occurrences to unit OSB/576 FLTS/DOX. Unit OSB/576 FLT/ DOX will then submit reports per CJCSI 3260.01 which is promulgated in the EAP-STRAT Vol 16 and concurrently notify 20 AF/A3NB and AFGSC/A3ON via chain of command. Ensure notifying 20 AF and AFGSC/A3ON does not impede PCC reporting timelines per CJCSI 3260.01. PCC and PCTT reporting requirements are due to the time-critical nature of the possibility of compromise. NSA personnel have access to UL timing studies, which detail how much time a potential adversary would need to take advantage of a temporary weakness in the safety and security of the ICBM weapon system. Code change actions required in the event of an actual compromise are provided in EAP-STRAT Vol 16, classified Annex A. **(T-0)**

9.2. Possible Code Compromise (PCC). Declaring a PCC indicates an unusual occurrence with ICBM code(s) or code component(s) and the circumstances need to be evaluated. Immediately contact USSTRATCOM/J374 when a situation meets PCC criteria. Units are directed to follow CJCSI 3260.01 reporting instructions, which is promulgated in the EAP-STRAT Vol 16, and concurrently notify 20 AF and AFGSC/A3ON via chain of command. Ensure notifying 20 AF and AFGSC/A3ON does not impede PCC reporting timelines per CJCSI 3260.01. **(T-0)**

9.3. Possible Compromise of TDI Technology (PCTT). In the event of a PCTT, numerous actions must take place in order to ensure the integrity of the ICBM weapon system. Declaring a PCTT indicates an unusual incident with holographic TDI(s), and the circumstances need to be evaluated. Immediately contact USSTRATCOM/J374 when a situation meets PCTT criteria. Units are directed to follow CJCSI 3260.01 reporting instructions, which is promulgated in the EAP-STRAT Vol 16, and concurrently notify 20 AF and AFGSC/A3ON via chain of command. (This does not apply to the 377 TEG). Ensure notifying 20 AF and AFGSC/A3ON does not impede PCTT reporting timelines per CJCSI 3260.01. **(T-0)**

9.4. COMSEC Incident Report. A COMSEC Incident Report is submitted per TO 00-33B-5508 if COMSEC material or equipment is involved. This includes all operational, test, training, and exercise COMSEC items identified by short title. If the incident involves TPC COMSEC material, the report is classified Secret. Classify incident reports involving non-TPC COMSEC material according to content. If the material is part of COMSEC account 613202, OSB will forward the report to USSTRATCOM/J374.

9.5. DULL SWORD Reports. DULL SWORD reports are submitted through the Safety Office. The Wing Safety Office should be contacted during incidents for coordination. All DULL SWORD reports drafted as the result of a PCC and containing details of the same are classified SECRET at a minimum.

9.6. Termination of MCCM Rest. Termination of MCCM rest will be IAW AFI 91-114. OSB will notify the wing of crew rest termination requirements. J374 will notify Wing OSB when the active PCC/PCTT has been resolved and crew rest may resume.

Table 9.1. Areas Affected During PCCs and PCTTs.

Component(s) Involved	Terminate Crew Rest for Affected Areas
DTU containing PEN D LFLCD data	Flight
P-Plug	Flight
DTU containing Complete Load or Code Change	Flight
CCV	Flight
Launch-Coded MGS or Computer	Flight
LFLCD-Coded MGS or Computer	Flight
OPS-Coded CSM(M)	Flight
Launch-Coded WSP	Squadron
LCP	Squadron
LEP	Squadron
TSEC/KS-60 (LF/LCC)	Squadron
WSP Exposed to C(a)C(b) Control Words	Squadron
J-Coded Components	Squadron
Holographic TDIs	Wing
Translate-Coded WSP	All Operational ICBM Units

Chapter 10

TRAINING AND EVALUATION REQUIREMENTS

10.1. Responsibilities.

10.1.1. Supervisors. Supervisors are responsible for ensuring all code handlers under their supervision accomplish the training required by this instruction. To request supplemental training, notify the Chief Training Officer (MX) or applicable unit Chief, Weapons and Tactics (OPS) when subordinates demonstrate a lack of code handling knowledge or proficiency.

10.1.2. Scheduling. All code handlers will be scheduled for codes training, as required. Scheduling of these individuals will be the responsibility of the member and/or the appropriate scheduling section. It is the member's responsibility to ensure they are scheduled for the appropriate training to meet currency and proficiency requirements. The codes training section will coordinate schedules to ensure training availability for members.

10.2. Codes Instructors. The SCC/FC will designate, in writing, OSB personnel to act as codes instructors for code handler classroom instruction. Only code controllers will be designated for code controller classroom instruction and WCPS instruction. Operator training will be accomplished only by SCC/FC-appointed instructors. Individuals selected as instructors must demonstrate a high degree of knowledge and proficiency.

10.2.1. The SCC/FC may be considered instructor qualified, regardless of AFSC prefix. However, they must maintain the same requirements identified for codes instructors.

10.2.2. Training Requirements. The Chief Training Officer must complete a 20 AF approved instructor training course. Prior instructor experience is desired but not required. Instructor training completed prior to appointment may be used to fulfill this requirement if the course is a 20 AF approved instructor training course. The OSS/CC or 576 FLTS/CC may grant a waiver to appoint the Chief Training Officer prior to instructor course attendance; however, attendance is required at the first available opportunity.

10.2.2.1. At a minimum, all codes instructors must receive instruction on the following items prior to certification: applicable equipment configuration, pre- and post-training scenario activities, local requirements, documentation requirements, classroom presentation to include audio/visual aids and instructor etiquette, construction and administration of knowledge tests, training materials, and lesson plans.

10.2.3. Missile squadrons will bring in Subject Matter Experts where appropriate. Only instructor qualified code controllers will teach codes-related topics in the classroom environment. Only instructor qualified code controllers are authorized to conduct initial codes training (ICT), Basic Mission Training (BMT), special training (in coordination with affected squadron), or code controller training.

10.2.4. Instructors presenting codes training will be knowledgeable of training methods and techniques, including lesson plan preparation, examination construction, classroom presentation, and deficiency analysis. Instructors must also be fully qualified on the Task ID being presented.

10.2.4.1. All instructors must complete a 20 AF approved instructor training course, to include the requirements in [paragraph 10.2.2.1](#) of this publication. Instructor training

courses completed in another position may be used to fulfill this requirement with the concurrence of 20 AF/A3NB and approval of AFGSC/A3ON. The OSS/CC or 576 FLTS/CC may grant a waiver to appoint codes instructors prior to 20 AF approved instructor course attendance; however, attendance is required at the first available opportunity.

10.2.5. Code Controller Instructor Recurring Training Requirements: Conduct instructor recurring training at least quarterly. Ensure instructor training covers all Task IDs identified in RCPTM for presentation during the quarter. OSB/576 FLTS/DOX instructor quarterly training will consist of all Task IDs identified in RCPTM for presentation during the identified quarter; additionally, Task ID I28 and subtasks will be accomplished.

10.2.5.1. Instructor quarterly training will be accomplished prior to the first presentation to the students of the identified Task IDs. The SCC/FC or Chief of Training will observe each certified code controller instructor conduct a training scenario/session at least every six months and document the observation in the individual's Individual Qualification Folder (IQF). The SCC will observe the Chief of Training at least every six months and document in the individual's IQF.

10.2.5.2. Document code controller instructor recurring training and observations and retain for 12 months within the individual's code controller folder.

10.3. Training Materials.

10.3.1. At a minimum, all training material must be coordinated with the appropriate safety office (i.e., Wing, NAF, or MAJCOM). Coordinate training material affecting or influenced by areas outside of ICBM Codes (e.g., Emergency Action Procedures, security response requirements, etc.) with Subject Matter Experts (SME).

10.3.2. The Chief Training Officer approves all OSB training materials. When the Chief Training Officer is absent, the SCC/FC may designate a certified code controller instructor to approve training products. Changes to the Code Handler Orientation Package (CHOP) and Familiarization (FAM) training may only be made by the Chief Training Officer. When the Chief Training Officer is absent, changes to the unit CHOP and FAM must be approved by the designated code controller instructor.

10.3.3. Unit Chief Training Officer will coordinate on and develop a training plan (TP) to meet the applicable task areas and events listed in the RCPTM. TPs will not contradict 20 AF/A3NB or AFGSC/A3ON guidance.

10.3.3.1. TP Content. The TP will include all applicable task areas and events listed in RCPTM. Those areas applicable to only OPS or MX code handlers may be specified. Its purpose is to provide a useful teaching tool that explains the subject area/task and governing directives associated with the subject area/task.

10.3.4. Lesson Guides. A lesson guide is required for each training activity. Lesson guides must be prepared and verified current before each training session.

10.3.4.1. Content. Lesson guides identify the title, objective, time required, materials, date prepared, and author. The lesson guide references the applicable portion of the MLP and/or appropriate directives or instructions. It must contain sufficient detail to identify the subjects being taught.

10.3.5. Instructional Aides. Instructional aides are used to increase the effectiveness of the training program. These include pictorial representations, test or training code components, task performance demonstrations, and devices in order to provide the student with a clear understanding.

10.3.6. Code Handler Orientation Package (CHOP). Creation of a CHOP is optional for the units and may be used to replace individual self-study packages. The CHOP identifies the self-study requirements for code handlers, code controllers, and BMC qualified individuals. The CHOP will include an in-depth explanation of all Task IDs. The self-study package may consist of references to required Task IDs within the CHOP with augmentation for specific information, as required. The CHOP may include a question portion to verify understanding. Scenarios are encouraged. If an update is required units can issue an interim change for the affected material to its personnel. Once a unit has completed self-study packages for all training sessions, they may combine them into one self-study and label it as the CHOP.

10.4. Code Handler Training (This does not apply to 377 TEG).

10.4.1. Code handler training will provide each handler with the knowledge necessary to build proficiency in order to properly control ICBM code components. The basis for ICBM Operator handler training is the Ready ICBM Program Tasking Memorandum (RTM). The basis of MX and OSB code controller training is the ICBM MX and OSB code handler Task ID list in RCPTM. Code handler training consists of four types: initial, recurring, individual, and special.

10.4.2. Documentation. Completion of initial, recurring, individual, and special training (BMT, etc.) will be documented in the current system of record. Retain documentation for 12 months.

10.4.3. Initial Codes Training (ICT). The purpose of ICT is to prepare individuals for code handler duties. Chief Training Officer will develop and conduct instruction on code control procedures contained in this and other associated publications. ICBM OPS, MX, and OSB personnel must successfully complete ICT on all Code Handler Task ID areas in RCPTM before their appointment and certification as code handlers.

10.4.3.1. ICT completed at another unit may be used to fulfill this requirement with an approval memo signed by the SCC/FC.

10.4.3.2. OSB will document initial training on the AFGSC Form 165. The SCC/FC will sign block I of the AFGSC Form 165 or concur with the signing authority in block I that a code handler has successfully completed all requirements. Signing authority for block I of the AFGSC Form 165 includes: the SCC/FC, Stan/Eval, Chief Operations Officer, Chief Training Officer, Superintendent, or individuals designated by SCC/FC memo.

10.4.3.3. For ICBM Operator code handlers, OSB will additionally submit the AF Form 1522, *Aviation Resource Management System (ARMS) Additional Training Accomplishment Report* for the appropriate RTM Event ID to the Squadron Aviation Resource Management (SARM) office to document ICT completion in Aviation Resource Management System (ARMS).

10.4.3.4. Code handler candidates will not be certified prior to successful completion of ICT in its entirety.

10.4.4. Recurring Codes Training. Code handler recurring training is to maintain handler currency and knowledge necessary to build proficiency in concepts and procedures.

10.4.4.1. Initial training counts as recurring training for the quarter in which it is completed. All code handlers receive recurring training quarterly. ICBM Operator code handler recurring training will be conducted IAW the published RTM and AFGSCI 13-5201V1, *Rapid Execution and Combat Targeting (REACT) Crew Training and Certification*. ICBM MX and OSB recurring training includes self-study packages identifying specific Task IDs and classroom training. Computer Based Training (CBT) methods may be used to satisfy recurring self-study requirements.

10.4.4.2. Recurring training includes new or changed concepts and procedures applicable to code handling duties, identified deficiencies, reportable code events, and other areas deemed necessary by the unit and 20 AF/A3NB. The inclusion of classified training materials during recurring training (e.g., PCC reports, PCTT reports) will be at the discretion and responsibility of the instructor to ensure the venue is cleared for classified material.

10.4.4.3. The Chief Training Officer will ensure self-study requirements have been met prior to receiving recurring training through trainee's attendance roster. MX code handlers and OSB code controllers must receive, as a minimum, annual training on all subject areas in RCPTM tables as applicable.

10.4.4.4. Restricted Status. The term "restricted" is synonymous with "inactive" in this document. ICBM Operator code handlers will be restricted IAW the RTM and AFGSCI 13-5201V1 & 2. MX individuals who fail to complete their proficiency requirements will be declared restricted by the SCC/FC. The SCC/FC will notify MX leadership of changes to status. The SCC/FC will remove the individual from restricted status after corrective training actions are completed with an instructor. Events accomplished for this restoration may count towards the member's cumulative proficiency event for the new training cycle. ICBM Operators will be in "No-Go" Status if they do not meet proficiency requirements.

10.4.5. Individual Training. The purpose of individual training is to enhance the individual's codes knowledge and proficiency. Individual training is conducted when serious deficiencies or lack of understanding are identified.

10.4.6. Special Training (ST). Special Training is developed, conducted, and documented under the supervision of a certified instructor to train handlers on new/changed procedures, hardware, software, and significant upcoming events (Simulated Electronic Launch Minuteman (SELM), Operation OLYMPIC STEP, etc.). ST will be developed by OSS based on the operational impact(s) of the new or changed procedure(s), hardware, or software. All training products involving codes must be coordinated through OSB/576 FLTS/DOX prior to training.

10.4.6.1. All code handlers involved with Operation OLYMPIC STEP will receive training on code change procedures, controls, and weapon system reactions prior to dispatching on any code change action.

10.4.7. Codes Familiarization Training (FAM). Codes FAM training self-study packages are developed by the Chief Training Officer to inform base personnel of code controls and procedures applicable to their areas of responsibility. If directed by the Wing Commander,

codes familiarization self-study packages or other media format (slide show or video) will be made available to ancillary agencies for employment in their unit training programs. The 576 FLTS/DOX is exempt from conducting FAM training.

10.4.7.1. If directed by the Wing Commander, units and ancillary agencies will ensure codes familiarization training for their members is accomplished prior to Operation OLYMPIC STEP.

10.5. Code Controller Training. The purpose of code controller training is to provide each code controller with the knowledge and proficiency necessary to properly control ICBM code components. In addition, code controllers are knowledgeable and proficient in the use of the WCPS and development of ground, flight, and targeting materials. The basis of all code controller training is the ICBM MX and OSB code controller Task ID List in the RCPTM. Tasks or subtasks trained by outside agencies may be certified as complete if all requirements have been satisfied (e.g., Two Person Concept (TPC) training administered by Current Operations Training). Code controller training consists of four types: initial, recurring, individual, and special.

10.5.1. For individuals transferring between bases, credit may be accepted for previously trained Task IDs. The losing SCC/FC will provide a Memorandum for Record (MFR) identifying Task ID coverage and annual expiration date to the gaining SCC/FC. This letter will include Holographic TDI pattern and identification of inspection level exposure (this does not apply to 576 FLTS/DOX). Additionally, the gaining SCC/FC will accomplish an MFR waiving the initial training requirement to be placed in the individual's training record, if prior Task ID coverage is deemed acceptable by the SCC/FC with the recommendation of the Chief Training Officer.

10.5.1.1. Individuals returning to a code controller position or being transferred as a code controller from one unit to another must re-accomplish initial code controller training if more than one year has lapsed since becoming inactive.

10.5.1.2. **[377 TEG Only]**. Code Controllers will retain training currency as described in [paragraph 10.5.1.1](#) even if member was decertified as a result of a PCS. Any code controller that does not meet the training currency requires initial code controller training.

10.5.2. Initial Training. Initial code controller training consists of code handler and code controller Task ID subject areas. Code controller selectees must complete initial code handler classroom training, if previous Task ID exposure was greater than 1 year prior, before beginning training on code controller Task ID tasks. Initial code controller training will count as recurring training for the quarter in which the code controller was certified. Individuals undergoing initial code controller training are considered Non-Mission Ready (NMR) until certified.

10.5.3. Shielded Enclosure (SE)/WCPS Training requirements.

10.5.3.1. Control of the WCPS and SE area must be maintained at all times IAW EAP-STRAT Vol 16. **(T-0)**

10.5.3.2. "Hands-on" training is the primary method of instruction for SE/WCPS tasks; therefore, make maximum use of test code components and devices. Observation of operational tasks will not satisfy "hands-on" requirements for a code controller.

10.5.3.3. At no time will the performance of a training task place the control of code components or materials at risk of a reportable possible compromise situation. If the supervising instructor feels that actions would result in a “real-world” situation they will immediately direct the team to cease all actions, provide corrective measures and inform the SCC/FC of the situation once proper control is established. The SCC/FC will make a determination regarding the continuation of training activities.

10.5.3.4. WCPS Initial Training. The purpose of initial WCPS training is to familiarize and train code controller selectees on the operation of the WCPS, exposing these individuals to specified Task IDs which require “hands-on” exposure. WCPS Initial training for non-certified code controllers will be conducted under the direct supervision of a WCPS instructor qualified in the task performed.

10.5.3.5. WCPS Recurring Training. WCPS recurring training will be conducted quarterly. All code controllers will remain current through the performance of operational/test WCPS coding in that quarter. Training will be captured in the Operator Operations Record and documented in the individual’s Operator Training Folder or in the Quarterly Training Folder by the Chief Training Officer. Changes to WCPS operations or procedures will be addressed with a supplemental lesson plan prior to operation of the WCPS. WCPS recurring training will be “hands-on” as much as possible. Operational/mission coding requirements may be used for recurring training as long as it is done with proper supervision by an OSB/576 FLTS/DOX instructor.

10.5.4. Individual Training. The purpose of individual training is to enhance the individual’s codes knowledge and proficiency. Individual training is conducted when serious deficiencies or lack of understanding are identified. Any qualified codes instructor can recommend code controllers for individual training. An evaluation resulting in a critical deviation will require individual training. The SCC/FC will identify the individual as requiring individual training and direct the development of a lesson plan. Individual training is conducted under the supervision of an OSB/576 FLTS/DOX instructor. The Chief Training Officer will document individual training in the individual’s code controller training folder.

10.5.4.1. Format. The type and extent of training will be determined by the codes training officer. The name and date of training will be included in the lesson guide for individual training.

10.5.5. Special Training. When new training requirements are established, each code controller will be trained and qualified in the task(s). These new tasks will be trained within 60 days following written notification of the task identification from AFGSC/A3ON. Code controllers must be qualified on the WCPS task(s) before performing WCPS task(s) unsupervised.

10.5.6. All Task ID training will be documented. Documentation must identify specific Task IDs and dates completed. Initial and individual Task ID training can be documented in the individual’s training record. Recurring training will be documented in Quarterly Training Folders.

10.5.6.1. Enlisted code controller training documentation is accomplished using myTraining, for each enlisted code controller. After all training is certified on the Individual Training Plan (ITP) in myTraining and Initial Task ID List Tracking Sheet

recurring training begins. Recurring training will be documented in the individual's training record.

10.5.7. Training Analysis. Analysis of the OSB training program and of MX/OSB individual codes proficiency is documented by the Chief Training Officer and is used to validate training. This analysis will include areas identified as requiring additional attention/instruction and recurring training/field deviations related to a Task ID.

10.6. Inactive Status. Code handlers and code controllers who fail to remain qualified IAW the requirements of this instruction and the RCPTM (the AFGSCI 13-5201V1 and RTM for ICBM Operator code handlers) are placed in inactive status. Persons are placed in inactive status for training, administrative or proficiency deficiencies.

10.6.1. Inactive (NMR) Status. The term "restricted" is synonymous with "inactive" in this document. Code controllers who fail to successfully complete recurring training during a given quarter are placed in inactive status at 0001L on the first day of the following quarter by the SCC/FC. Once the recurring training actions are complete and the individuals are no longer delinquent in meeting the requirements, they may be returned to active status.

10.6.1.1. The OSS/CC may place code controllers into inactive status if needed for corrective training. The OSS/CC may elect to have the individual complete certification briefing, directed retraining, and/or WCPS evaluation to return to active status.

10.6.2. Inactive status is documented in the training system of record. The 576 FLTS/DOX may use an appropriate alternative method for tracking inactive status.

10.6.2.1. Individuals placed in inactive status are not allowed to perform code handler/code controller duties until the reason for their inactive status has been corrected. Persons who remain in inactive status for more than two consecutive quarters due to failure to receive training will be decertified.

10.6.2.2. To ensure inactive code handlers/code controllers are not scheduled to perform duties, the OSB/576 FLTS/DOX Training Officer provides base agencies with the names of code handlers and code controllers placed on inactive status for failure to complete codes training.

10.7. Code Controller Individual Qualification Folder (IQF). Maintain individual training folders for each code controller until decertification. These folders must include:

10.7.1. AFGSC Form 165, Code Handler Certification and Training Record (Part III signed).

10.7.2. AFGSC Form 166, Code Controller Certification and Training Record (Part I and II signed). This form is not applicable for code controllers certified prior to 11 April 2017. Prior to 11 April 2017, an AFGSC Form 165 with the duty title of "Controller" is acceptable.

10.7.3. Evaluation and training documentation.

10.7.4. Approval for code control group reassignment, if applicable.

10.7.5. Documentation of assignment to their current duty.

10.7.6. Appointment letters (e.g., Instructor, Stan/Eval, Evaluator), SME, etc.

10.7.7. Documentation of attended courses (i.e., Basic Instructor Course, etc.) and other miscellaneous information.

Chapter 11

CODE CONTROLLER EVALUATIONS

11.1. SCC/FC Responsibilities. The SCC/FC establishes and implements the Quality Assurance and code controller standardization and evaluation programs. The overall goal of these programs is to provide commanders with meaningful indicators reflecting the effectiveness of code controller training and the ability to perform the unit mission.

11.1.1. The SCC/FC will appoint the Stan/Eval and an alternate evaluator (if desired) and will maintain written certification/appointment in the individuals' code controller folder.

11.1.2. The SCC/FC is responsible for the management and maintenance of a codes certifying official's qualification program. This program will be used to ensure qualified individuals are certified in the positions requiring code handler status and code controller duties.

11.1.3. All individuals designated under the codes certifying official's qualification program for handler certification will be current on Task ID **I27** (with the exception of SQ/CC/DO). Responsibility for management of the codes certifying official's qualification program may be delegated to the Stan/Eval.

11.2. ICBM Code Controller Standardization/Evaluation Officer Certification.

11.2.1. Training. The Chief of Stan/Eval must complete a 20 AF approved evaluator training course. Prior evaluator experience is desired but not required. Evaluator training completed prior to appointment may be used to fulfill this requirement as long as the course is a 20 AF approved evaluator training course. Each OSB/576 FLTS DOX will develop a local initial and recurring Stan/Eval training program. Initial training will be completed prior to certification as the Stan/Eval. Recurring training is required annually on appropriate evaluator-related Task ID tasks.

11.2.1.1. As a minimum, this program will cover planning and supervising an evaluation program, conducting an evaluation, preparing evaluation scripts, and maintaining evaluation records. These tasks are identified in the ICBM Operator Task ID List.

11.2.1.2. The 20 AF/A3NB will provide units with additional guidance, as required.

11.2.2. Certification. The following establishes the certification process for the Chief of Stan/Eval and designated alternate evaluator.

11.2.2.1. Prior to certification, the incumbent Chief of Stan/Eval or designated alternate evaluator will administer a recurring evaluation to the incoming Stan/Eval appointee. The incumbent Chief of Stan/Eval or designated alternate evaluator will observe the Chief of Stan/Eval appointee conducting an evaluation. Once the SCC/FC is satisfied that the Stan/Eval has completed all training requirements, the SCC/FC will certify the new Stan/Eval.

11.2.2.2. Document certification in the individual's training record and identify the individual on the code controller listing memorandum. This consists of documenting that the individual has completed required training and is qualified to perform duties as Stan/Eval or designated alternate evaluator and has been approved by the SCC/FC.

11.2.2.3. AFGSC/A3ON or 20 AF/A3NB may perform recurring evaluations utilizing a QCO of the Stan/Eval for all 20 AF units (AFGSC/A3ON for 377 TEG) to ensure the individual is qualified and proficient in their duties, if required. If a QCO was utilized for a recurring evaluation of the Stan/Eval it must meet all recurring evaluation requirements as defined in this chapter. AFGSC/IG, AFGSC/A3ON, 20 AF/A3NB may also observe the Stan/Eval conducting an evaluation during SAV and/or HHQ inspections.

11.2.2.4. The Stan/Eval must maintain currency on all WCPS training requirements.

11.2.2.5. The SCC/FC may be considered evaluator qualified but must maintain the same requirements identified for code controller evaluations.

11.3. Evaluations.

11.3.1. All code controllers will be evaluated within 18 months of their initial certification evaluation or last recurring evaluation. Any code controller who is not evaluated within the 18-month period will be placed on inactive status on the first day of the 19th month until a recurring evaluation is conducted.

11.3.1.1. **[377 TEG Only]**. Code controllers will retain evaluation currency as described in [paragraph 11.3.1](#) even if member was decertified as a result of a PCS. Any code controller that does not meet the certification currency will require an initial evaluation, regardless of training currency status.

11.3.2. AFGSC/IG, AFGSC/A3ON, or 20 AF/A3NB may use on-line unit scripts with associated problem cards or QCOs during unit visits.

11.3.3. At a minimum all evaluation material must be coordinated with the appropriate safety office (i.e., Wing, NAF, or MAJCOM). It is encouraged that evaluation material affecting or influenced by areas outside of ICBM codes (e.g., Emergency War Order Procedures, Security response requirements, etc.) are coordinated with the Subject Matter Expert.

11.3.4. Evaluation Types. There are three types of evaluations: initial, recurring, and requalification. Task coverage for each evaluation must contain the minimum tasks required to meet the objective of the evaluation (e.g., coding an LCP). These evaluation types fall into two categories: Test and Operational. Initial and requalification evaluations will only use test codes (i.e., test data disk). Recurring evaluations may use test or operational codes if pre-existing requirements (e.g., scheduled MGS R&R) for status presentation are scheduled. Use of operational codes for recurring evaluations is at the discretion of the Stan/Eval.

11.3.4.1. Initial Evaluation. An initial evaluation is given upon completion of NMR code controller training and required for code controller certification. An initial evaluation should be modified to “isolate” the code controller(s) being certified. The code controller(s) being certified should direct all actions during the evaluation. Individuals supporting an initial evaluation will be given credit for a recurring evaluation.

11.3.4.2. Recurring Evaluation. A recurring evaluation is a periodic evaluation of a Mission Ready (MR) code controller designed to determine proficiency and capability to support the mission. A Quality Control Observation (QCO) can be utilized for a recurring evaluation if it meets all recurring evaluation and QCO requirements as defined in this publication. See [paragraph 11.3.4.4](#) of this publication for more details.

11.3.4.2.1. Recurring evaluations may utilize problem cards to prompt response to emergency procedures when no other operational actions are pending. The problem card presented, or verbal question, will be documented on the evaluation report.

11.3.4.2.2. If operational codes are utilized, the components will be secured or issued prior to evaluation injects.

11.3.4.3. Requalification Evaluation. Requalification Evaluations are given as a result of a Qualification Level 3 (Q3) rating or an operational impacting deviation at the discretion of the SCC/FC. As a minimum, retraining and reevaluation must address the action resulting in the Q3 rating or operational impacting deviation and be documented in the member's record. In addition to requalification training, the SCC/FC may identify the need for a requalification evaluation.

11.3.4.3.1. A requalification evaluation may be a complete evaluation, but at a minimum, it must evaluate those tasks that resulted in the unqualified rating.

11.3.4.3.2. The code controller(s) being re-evaluated must direct all actions during the evaluation. Any remaining code controller team member(s) will accomplish all actions as directed and will receive recurring evaluation credit if the requalification evaluation is a complete evaluation.

11.3.4.4. Quality Control Observation. QCOs are observations of code controllers in the performance of their normal duties to provide additional performance feedback to the SCC/FC. Any combination of vault, secure area or WCPS operations may be observed. QCOs are performed at the discretion of the SCC/FC.

11.3.4.4.1. QCOs must utilize pre-existing requirements (i.e., scheduled MGS R&R) for status presentation. Simulated status or question(s) (unless to clarify an action) will not be introduced during the operational portion of the QCO.

11.3.4.4.2. QCOs shall utilize only operational codes unless pre-existing coding requirements (i.e., scheduled HSEP, 377 TEG) require the use of test codes.

11.3.4.4.3. QCOs may be utilized for recurring evaluations as long as all recurring evaluation requirements are met as defined in this chapter.

11.3.4.4.4. Termination of a QCO is at the discretion of the Stan/Eval.

11.4. Script Requirements.

11.4.1. Each OSB/576 FLTS/DOX must develop scripts for use during evaluations. OSB/576 FLTS/DOX will keep a minimum of two initial scripts online. The Stan/Eval will determine the Task ID(s) to be covered in each script. However, with the exception of requalification evaluation scripts, each script must contain the minimum requirements to meet the objective of the task being evaluated (e.g., coding an LCP or LEP, etc.).

11.4.1.1. Units are authorized any additional scripts (initial or recurring) at the discretion of the SCC/FC.

11.4.2. Scripts must be technically accurate. Scripts must provide a presentation plan of problem sequences and events that specify instructions for the evaluator and identify proper code controller team responses. Scripts may contain oral questions.

11.4.2.1. The evaluator should follow the script as written unless a deviation is required to provide accurate status. Problems that do not lend themselves to sequential operation should be avoided, if possible.

11.4.2.2. Units will number and date scripts and individual problem cards, as required, to facilitate control and use, and file them in a manner to preclude disclosure to team members subject to evaluation.

11.4.3. Scripts may utilize problem cards to prompt response to emergency procedures when no other operational actions are pending. The problem card presented, or verbal question will be documented on the evaluation report. It is at the discretion of the evaluator to determine if demonstration or verbal response fulfills the requirement. The desired response must be provided to the evaluatee (i.e., “For evaluation purposes, please demonstrate/describe how you would respond to the situation presented”).

11.4.4. Script Content and Design. Procedural entering requirements specified in technical orders and other directives must be reasonably apparent. They must not be “masked” in order to present a theoretically possible, but improbable, occurrence. “Masking” means using one element of status to suppress another element of status to the extent that the second element of status is not easily detectable. This does not mean presentation of simultaneous problems.

11.4.5. Performance. Scripts can measure performance in non-WCPS duties and WCPS operations. WCPS operations can include peacetime or force generation scenarios. All scripts, with the exception of requalification evaluation scripts, must comply with minimum requirements defined below.

11.4.6. Script Minimum Requirements:

11.4.6.1. At a minimum scripts will contain a reporting and emergency response capability/procedures (**Task ID I25**); do not evaluate **I25C** or **I25D**.

11.4.6.2. At a minimum scripts will demonstrate split handling control concept (i. e., proper control of WCPS).

11.4.6.3. At a minimum one of the “R” coded items in the AFGSC Ready Codes Program Tasking Memorandum (RCPTM) must be directed and accomplished by the individual under evaluation.

11.4.6.4. Inherent tasks are actions that are typically accomplished in every evaluation. These tasks occur naturally in order to accomplish another Task ID. These Task IDs will be listed in each script as inherent Task IDs.

11.4.7. Script Approval. The SCC/FC must coordinate and approve all WCPS scripts used for evaluations. The coordination and approval will be documented. For a script that will be administered to the SCC/FC, the OSS/CC or 576 FLTS/CC/DO will provide this function.

11.4.8. Units must retain evaluation scripts and ancillary items such as dispatches, status cards and script programming, in either paper or electronic copy, for a period of at least 12 months from the off-line date. This does not require a removable storage element for old revision products. Off-line scripts do not require updates.

11.5. Evaluation Conduct.

11.5.1. Evaluation Preparation. Below are the minimum required preparatory actions; their sequence may vary.

11.5.1.1. The evaluator must prepare and review the selected script and associated materials.

11.5.1.2. The evaluator must initiate a code controller's AF Form 8 for each code controller to be evaluated.

11.5.1.3. For initial evaluations the evaluator(s) (e.g., Stan/Eval) may serve as part of the TPC team. The evaluator will not serve as a member of the TPC team, nor provide control over components or code materials, during recurring evaluation. In the event of an emergency that requires the evaluator to serve in this capacity when working with operational material, the evaluation will be immediately suspended or terminated.

11.5.1.4. For evaluations with two non-certified members, members should be of the opposite control groups and accomplish an individual tasking directly associated with their control group.

11.5.1.5. Stan/Eval shall not expose an evaluatee to the same script two evaluations in a row. The Stan/Eval will look at previous evaluation documentation of the evaluatees prior to determining which script to administer.

11.5.2. Evaluation in-brief. Evaluators conduct an evaluation in-brief to ensure all members of the evaluatee code controller team, on-duty shift code controllers, and support personnel understand the rules of engagement. The in-brief sets the environment for the evaluation and must clarify the level of support/non-support to be given. The in-brief will cover the following areas:

11.5.2.1. Evaluator-evaluatee relationship.

11.5.2.2. Methods used to initiate events (e.g., problem cards, telephone calls, real-world activity, and equipment indications). All script inputs must be clearly identified as exercise inputs.

11.5.2.3. Responsibilities during equipment operations.

11.5.2.4. Safety policies.

11.5.2.5. Responsibilities during actual emergencies, malfunctions, or real-world events.

11.5.2.6. Status of evaluators in terms of PRP and code-handling restrictions.

11.5.3. Use of test versus operational codes.

11.5.3.1. Test codes should be used as much as possible; however, if an operational requirement exists, operational codes may be used in a recurring evaluation, if it satisfies the Task ID(s) coverage in the script.

11.5.3.2. Operational codes will never be used in an initial evaluation or requalification evaluation.

11.5.4. Conducting the Evaluation. The evaluator will present status in accordance with the script, then observe and document the team's response to that status and all actual WCPS status.

In an evaluation, an agency would not do more than is required by regulation or applicable technical order.

11.5.4.1. Failing to accomplish any required action is always a deviation or critique item. The evaluator should not hesitate to document deviations for these incidents. An evaluator may document a deviation for lack of proficiency in performing a task using sound professional judgement in assessing the degree of deviation and guidance in accordance with this publication.

11.5.4.2. The evaluator will not permit any deviation to evolve into a real-world possible code compromise, PCTT, WSSR violation, TPC violation, or damage to codes-related equipment. **(T-0)**

11.5.4.3. If a task is not intended to be evaluated (or evaluated again after being previously accomplished correctly), brief the task accomplished when the team identifies the requirement to accomplish the task.

11.5.4.4. The evaluator must always provide status that team members would normally detect with their senses (e.g., heat, air, smoke, etc.) when it cannot be provided by the WCPS or SE support equipment. This may require the use of problem cards or a verbal announcement by the evaluator.

11.5.4.5. Ensure correct WCPS status is presented for briefed tasks.

11.5.5. Termination of Evaluations.

11.5.5.1. Ensure intended task coverage is achieved before terminating an evaluation. The script may call for termination at some point short of task completion if it is not intended to evaluate the remaining requirements (e.g., HDA coding). However, do not terminate an evaluation until the team has had an opportunity to complete all actions required by the script. An evaluation is not terminated prior to completion unless one of the subsequent condition(s) are applicable:

11.5.5.1.1. An evaluatee/evaluator is unable to perform duties due to injury, illness, etc.

11.5.5.1.2. “Real-world” maintenance activity or coding interferes with evaluation.

11.5.5.1.3. HHQ actions preclude completing evaluation.

11.6. Post-Evaluation.

11.6.1. Deviation Determination. Upon completion of the evaluation, evaluators will identify, assess, and document deviations.

11.6.1.1. Deviation determination must be based upon the actions or inactions of the evaluatee regardless of scripted events.

11.6.1.2. During a scenario, if a crew takes multiple incorrect actions that lead to an action warranting a more severe deviation, assess only the highest degree deviation, and fully describe the other incorrect actions in the deviation description (commonly referred to as snowballing).

11.6.1.3. Assess deviations to only one code controller when, at the evaluator's discretion, the other code controller was not in a position to detect and had no requirement to detect the incorrect action.

11.6.2. The SCC/FC is the final deviation determination authority based on input from the Stan/Eval. If there is a disagreement on a critical deviation, SCC/FC will query the deviation(s) to 20 AF/A3NB. The affected code controller(s) will not perform unsupervised coding operations until the SCC/FC receives a determination from 20 AF/A3NB. 20 AF/A3NB will provide the pass/fail scenario and determination to all units.

11.6.2.1. If it is not possible to determine how to assess a deviation for an ongoing evaluation after querying all required on-base agencies (e.g., OGV, Safety, Missile Maintenance Operations Center (MMOC), etc.), call and initiate a formal request for clarification with 20 AF/A3NB. The Stan/Eval will pass all information regarding the deviation and the associated scenario to 20 AF/A3NB who will analyze the information, make a final deviation determination, and respond back to OSB/576 FLTS/DOX as soon as possible. The final determination will be sent to all units.

11.6.2.2. Deviation Categories. Assess a deviation when an evaluatee performs an incorrect action. There are two types of deviations, critical and non-critical.

11.6.2.3. Critical Deviation. A critical deviation is an incorrect action which, in the judgment of the evaluator, would reasonably be expected to result in operational mission failure, endangerment of human life, serious injury, or death. A critical deviation results in the code controller being restricted and unqualified for all positions and receiving a Q3 rating. The code controller may not perform unsupervised operations duty until successful completion of a requalification evaluation. Some examples of critical deviations are as follows (this is not an all-inclusive list):

11.6.2.3.1. A violation of WSSRs pertaining to control and operations of ICBM codes components.

11.6.2.3.2. A critical code handling violation resulting in the loss of proper control, loss, or loss of proper security of an ICBM code component, including test codes components used for evaluation or inspection purposes.

11.6.2.3.3. A violation of TPC control or no-lone zone requirements.

11.6.2.3.4. Failing to accomplish a critical portion of a task that directly impacts the alert status of a launch facility or launch control center, or the proper operation or verification of a code component.

11.6.2.3.5. Failing to identify and correct a condition involving improper control of a code component.

11.6.2.3.6. Failing to identify and correct an incorrectly coded component.

11.6.2.4. Non-critical Deviations. Assess a non-critical deviation when incorrect evaluatee actions are not significant enough to meet critical deviation criteria. A non-critical deviation is an incorrect action which, in the judgment of the evaluator, would reasonably be expected to result in operational mission degradation or personnel injury. Some examples of non-critical deviations are listed below (this is not an all-inclusive list):

11.6.2.4.1. The inability to complete a task due to a lack of knowledge or proficiency.

11.6.2.4.2. A deviation that would result in equipment damage to a codes-related component.

11.6.2.4.3. A deviation which results when a critical portion of a task is re-accomplished when not required, including unnecessary dispatch or loss of dispatch, or preventing a launch-capable sortie from being placed on alert.

11.6.2.4.4. Failure to comply with warnings or technical order safety precautions that could reasonably be expected to result in endangerment of human life, serious injury, or death.

11.7. Evaluation Debrief. Following the evaluation, it is vital for evaluatees and evaluators to conduct a thorough debrief. The debrief provides an opportunity to conduct critical self-assessment in an effort to continuously improve.

11.7.1. Evaluatees will:

11.7.1.1. Accomplish a debrief following the evaluation. The SCC/FC and CRO should be available for assistance. Reference AFTTP 3-3 ICBM, Attachment 10, for recommended techniques and procedures.

11.7.1.2. Debrief all actions conducted during the evaluation to demonstrate knowledge of requirements and understanding of events performed during that evaluation phase. This will be conducted under the supervision of the evaluator and can be used to determine if retraining will be required.

11.7.2. Evaluators will:

11.7.2.1. Not add or remove deviations based on the debrief (e.g., if a crew self-identifies a deviation that the evaluator did not observe prior to the debrief, the evaluator cannot assess the deviation).

11.7.2.2. At the conclusion of the debrief:

11.7.2.2.1. Present noted deviations to the evaluatee(s) and determine if directed training is required. If directed training is not required, ensure instruction is provided IAW AFGSCI13-5201V2. If directed training is required (self-study not included), the highest possible rating for the code controller is a Q2.

11.7.2.2.2. Provide critiques, recommended focus areas for future training, and additional information as required.

11.7.3. The SCC/FC or designated representative may determine additional training is required for the evaluatee. This will not alter the AF Form 8.

11.8. Outbrief. Provides an opportunity for evaluators to brief the overall evaluation rating upon completion of all evaluation phases.

11.9. Evaluation Ratings. Overall evaluation ratings will be based on the discretion of the SCC/FC with input from the Stan/Eval.

11.9.1. Qualification Level 1 (Q1) indicates an evaluatee demonstrated the desired level of performance and knowledge of procedures, equipment, and directives within prescribed

tolerances. This will be awarded when no deviations are noted, but may also be awarded when deviations are noted if:

11.9.1.1. No critical deviations were noted.

11.9.1.2. In the judgment of the evaluator, any non-critical deviations noted do not warrant directed training nor preclude awarding of a Q1. At the conclusion of the debrief, the evaluator provides instruction concerning the deviation and determines that the examinee has gained the necessary knowledge or proficiency.

11.9.2. Qualification Level 2 (Q2) indicates an evaluatee demonstrated the ability to perform duties safely with no critical deviations. However, the evaluatee may have committed any of the following deviations or generally performed below Q1 standards. Initial qualification level determination rests with the evaluator:

11.9.2.1. There were one or more non-critical deviations where, in the judgment of the evaluator, directed training was assigned.

11.9.2.2. In the judgment of the evaluator, an evaluatee's performance of an action, although correct, requires directed training.

11.9.3. A Q3 rating indicates an evaluatee is unqualified based on an unacceptable level of safety, performance, or knowledge.

11.9.3.1. A Q3 will require code controllers be placed on inactive status until directed retraining and a requalification evaluation is accomplished for the deviation resulting in the unqualified rating. For enlisted code controllers, a new training and certification date will be entered into MyLearning, *On-the-Job Training - Continuation Sheet*. For officer code controllers, training records will be annotated to reflect the individual being restricted and placed back on active status once a recheck has been completed and passed.

11.9.3.2. A requalification evaluation including all events with a critical deviation is required.

11.9.3.3. In the judgment of the evaluator, a Q3 may be given if there is justification based on several non-critical deviations noted.

11.10. Evaluation Documentation. Administration of the code controller qualification evaluation program requires accurate documentation. This provides a means to document code controller readiness, identify deviation(s), and direct training as applicable. A code controller's initial evaluation and two most recent evaluation documentation will be retained in their IQF.

11.10.1. AF Form 8. An AF Form 8, *Certificate of Aircrew Qualification*, will be used for all evaluations and QCOs. Prior to date of this publication, Corrective Action Worksheets are acceptable. Units will use electronic signatures for any required signatures on Stan/Eval forms to the maximum extent possible. The AF Form 8 will be filed in the evaluation section of the IQF of the evaluatee. Use AFGSCI13-5201V2 as a guide to properly fill out the AF Form 8.

11.10.2. The AF Form 8s will be maintained in the individual's training/evaluation records until the individual is permanently decertified as a code controller. Records more than 5 years old for active code controllers may be moved to an archive section maintained by OSB/576 FLTS at the discretion of the SCC/FC but must be maintained until the individual is decertified and the wait period for destruction has lapsed. These records may be maintained through paper

or electronic means. When retraining is required, the OSB/576 FLTS Training Section will receive and maintain copies of the AF Form 8 for training purposes. The AF Form 8 coordination process should be accomplished expeditiously to ensure all individual records are kept current. Units will determine individuals involved in the AF Form 8 process. Individual records must maintain all restriction-related paperwork to include AF Form 8, restriction letters (to include a letter for removal from inactive status), and training documentation. Inspection teams are required to create an AF Form 8 for deviations identified during HHQ inspections/visits not addressed in the final report.

11.10.3. Evaluation details. Evaluation date, location, and no-notice applicability must be annotated.

11.10.3.1. Document all deviations and downgrades on the AF Form 8 driving a Q2 or Q3 rating. Note deviations which require directed training in Section VIII of the AF Form 8.

11.10.3.2. Expiration date information will be listed on the evaluation report even if there is no change (e.g., QCO).

11.10.3.3. An evaluation type must be listed for each individual:

11.10.3.3.1. Use an “I” to record an initial evaluation for code controller certification purposes.

11.10.3.3.2. Use an “R” to record a recurring evaluation or QCO. A recurring evaluation is a periodic evaluation of a team or team member designed to determine proficiency and capability.

11.10.3.3.3. Use an “S” to record a requalification evaluation that is a result of a previously failed evaluation. This type of requalification evaluation may be a complete evaluation or may only evaluate tasks that resulted in the unqualified rating.

11.11. Directed Training. All ratings of Q2 or Q3 require directed training. Directed training is any training directed by the evaluator to remedy deviations or crew performance identified during the evaluation.

11.11.1. Directed training may include classroom instruction, or use of the WCPS using test codes only.

11.11.2. Directed training and requalification evaluation resulting in a Q1 or Q2, associated with a Q3 rating, will be completed prior to accomplishing coding duties.

11.11.3. Document directed training on the AF Form 8.

11.12. Deficiency Reporting. When a team has performed normal coding actions (not under formal evaluation) and procedural deviations are observed or found through a review of WCPS printouts or configuration records and results in recoding or additional dispatches, the SCC/FC and CRO shall be notified in writing immediately after discovery. The SCC/FC shall determine corrective actions. Do not document as a critical deviation or non-critical deviation, but ensure the affected agency (i.e., MMOC, OSK, etc.) understands the severity of the deviations and required corrective actions.

Chapter 12

CERTIFICATION AND DECERTIFICATION

12.1. Code Handler and Code Controller Certification Program. The SCC/FC is responsible for the code handler/code controller certification program.

12.2. Prerequisites for Certification of Code Controllers and Code Handlers.

12.2.1. Before certification as a code handler or code controller, individuals must meet the prerequisites identified in EAP-STRAT Vol 16 and the following additional prerequisites:

12.2.1.1. Command Assignment. AFGSC or AETC military or DAFC personnel will serve as code controllers or code handlers at AFGSC units. Code controller and code handler selectees must have documentation assigning them to an ICBM unit prior to initial training and are prohibited from handling operational components. **(T-0)**

12.2.1.2. The unit SCC/FC will review each selectee record to identify potential certification limitations and provide their recommendation to the OSS/CC or 576 FLTS/CC prior to approval of PCA/PCS.

12.2.1.3. Security Clearance. Code handlers must have a final Top-Secret clearance based on CJCSI 3231.01, *Safeguarding Nuclear Command and Control Extremely Sensitive Information* requirements. Officer, enlisted, and DAFC code controllers and operations scheduling officer code handlers are authorized access to Top Secret Nuclear Command and Control Extremely Sensitive Information (NC2-ESI) as outlined in CJCSI 3231.01. **(T-0)**

12.2.1.4. Grade. Officer and enlisted code handlers can be in any grade. Officer code controllers are required to be a commissioned officer, enlisted code controllers in the grade of E-4 or above, and civilian code controllers in the grade of GS-7 or above with a minimum of 1 year of federal service (includes prior military service). Civilian code controllers will be considered officer code controllers when certified for the purpose of code control and handling. Code controllers will have 1 year of previous code handler/code controller experience prior to assignment to OSB/576 FLTS/DOX. Waivers for previous code handler/code controller experience will be determined by AFGSC/A3ON with recommendation from 20 AF/A3NB on a case-by-case basis and approved by AFGSC/A3ON.

12.2.1.5. Personnel Reliability Program (PRP). Code handlers and code controllers are required to be certified in a critical PRP position IAW DoDM 5210.42_DAFMAN 13-501, *Nuclear Weapons Personnel Reliability Program (PRP)*. **(T-0)**

12.2.1.6. Two-Person Concept (TPC) Team. Code handlers and code controllers must meet the team requirements for a TPC team. A two-person concept team consists of at least two individuals authorized by the commander and verified by their supervisor to meet the following requirements:

12.2.1.6.1. Are certified under the Personnel Reliability Assurance Program, as specified in DoDM 5210.42_DAFMAN 13-501. **(T-0)**

12.2.1.6.2. Know the nuclear weapons surety requirements of the task they perform.

12.2.1.6.3. Can promptly detect an incorrect act or unauthorized procedure

12.2.1.6.4. Are designated to perform the required task.

12.2.1.6.5. Unit code controllers and code handlers will receive TPC Training and initial and recurring nuclear surety training IAW DAFI 91-101.

12.2.1.6.6. Unauthorized Launch Studies Duty Restriction. Before certification, military and civilian code controllers and handlers must be screened for any previous access to an ICBM Unauthorized Launch Study (ULS) or Launch Activation Study (LAS). Individuals with prior or current access to ULS information are expressly prohibited from becoming a code handler, code controller or serving as part of a Two Person Concept team. An assignment limitation code (ALC) will be annotated in personnel records. **(T-0)**

12.2.1.6.6.1. Headquarters Air Force Personnel Center (HQ AFPC), upon notification from Headquarters Air Force Safety Center/Nuclear Weapons Safety (HQ AFSEC/SEWN), tracks who has or had access to ULS information and annotates official personnel records with ALC M. Reference DAFI 36-2110 for more information on ALC assignment. **(T-0)**

12.2.1.6.6.2. Prior to any assignment potentially requiring TPC qualification, HQ AFPC will screen personnel for an ALC M. If ALC M is noted, HQ AFPC will consult with HQ AFSEC/SEWN about the individual's access to UL information and any potential assignment impacts. **(T-0)**

12.2.1.6.6.3. The SCC/FC will interview candidates with previous ICBM (airborne or ground launch), Submarine Launched Ballistic Missile (SLBM), or ALCS experience to determine previous access to ULS information. Any personnel with ALC M must not have access to superseded, operational, or reserve codes or to have the opportunity to derive the Worldwide Unlock code. **(T-0)**

12.2.1.6.6.4. A waiver may be granted if the UL information relates to a different weapon. Send waiver requests to 20 AF/A3NB with an information copy to USSTRATCOM/J374 who will coordinate the waiver with AFGSC/A3ON. 20 AF/A3NB will determine the advisability of the waiver in coordination with DIRNSA/C62 and HQ AFSEC/SEWN. Make no exceptions and/or code certification without prior written approval from DIRNSA/C62 and HQ AFSEC/SEWN. **(T-0)**

12.2.1.6.7. Previous holographic TDI/code material access. For individuals that were previous code controllers, before an individual is allowed access to codes or TDIs, previous access to codes material, holographic TDI inspection procedures and control group must be verified. If an individual has had previous level 2 TDI Inspection Criteria access, units must verify the following with 20 AF/A3NB and AFGSC/A3ON with concurrence from USSTRATCOM/J374 **(T-0)**:

12.2.1.6.7.1. The member's duties will not provide them access to any current complementary code. **(T-0)**

12.2.1.6.7.2. Members with exposure to current world-wide unlock code/unlock values controlled under split-knowledge procedures will not receive unescorted

access to LFs or LCCs. **(T-0)**

12.2.1.6.7.3. Members with previous access to holographic TDI inspection procedures will not accomplish alert duties at a unit where the TDI pattern(s) they had access to are in use in LCCs. **(T-0)**

12.2.1.7. Training. Individuals must have completed an initial training program before certification as a code handler or code controller. **(T-0)**

12.2.1.8. Communications Security (COMSEC) Access Documentation. All code handlers and code controllers must be enrolled in the Cryptographic Access Program (CAP).

12.2.1.9. Ensure an SD Form 572 is completed prior to certification.

12.2.2. Inform the administering official of any situation that would require suspension or revocation of access. If suspension of access is required, the individual must be placed in inactive status until access is reinstated or the individual is decertified for code handling.

12.3. Code Handler Certification and Decertification (This does not apply to 377 TEG).

12.3.1. Individuals will not perform code handler tasks (to include alert, maintenance, field evaluations, or task performance involving operational code material), until they have been certified. Individuals must meet qualification and certification requirements before interaction with operational code material or the launch, enable, or encryption portion of the operationally configured weapon systems. Before certifying a former code controller as a code handler, comply with the EAP-STRAT Vol 16. Before certifying a previous code handler in the opposite control group, comply with EAP-STRAT Vol 16. **(T-0)**

12.3.2. Code Handler Certification.

12.3.2.1. The OG/CC or SQ/CC will certify personnel whose duties involve the control of code components as officer or enlisted code handlers. This certification is authorized based on coordination between the squadron commander or operations officer and the SCC/FC. The SCC/FC can perform code handler certification duties in lieu of the SQ/CC or OG/CC. A designated alternate may perform the certification/recommendation at the discretion of the SCC/FC. This must be designated by the SCC/FC in writing and kept until all documents with that individual's signature authority are no longer applicable. Appointees within OSB should be limited to Stan/Eval, training officer, or certified codes instructors.

12.3.2.2. As a minimum, certification includes a briefing covering code handling concepts, components/material, controls, incident reporting (PCCs, PCTTs, etc.), and a personal interview with the certifying official to ensure the provisions of the EAP-STRAT Vol 16 are met.

12.3.2.3. The CRO will ensure the base COMSEC manager is notified, and SD Form 572 is completed.

12.3.2.4. Code handler certification and decertification will be documented on the AFGSC Form 165. For ICBM Operator code handlers, OSB will additionally submit the AF Form 1522, *ARMS Additional Training Accomplishment Report* for the appropriate RTM Event ID to the Squadron Aviation Resource Management (SARM) office to document the codes certification date in ARMS. **(T-0)**

12.3.3. AFGSC Form 165. OSB will maintain the current AFGSC Form 165 on each code handler. The form is initiated when the individual begins codes training at the unit. Upon completion of initial training, the instructor or other authority IAW 10.4.3.2 of this regulation signs and dates Part I of the Code Handler Certification and Training Record. When all prerequisites are completed, the individual and certifying official sign and date Part II of the form. Once Part II is signed, the only authorized change to this form following certification will be due to a legal name change of an individual. If an administrative or clerical error is identified following signing of Part II, it will be documented utilizing a memorandum for record to be kept with the original document. For other changes (i.e., PCS/PCA with a certifying official change) a new AFGSC Form 165 will be completed re-using existing data from the original 165 at the discretion of the gaining OSB.

12.3.4. Decertification. Decertification of a code handler is not required due to PCA or PCS if all prerequisite requirements identified in this publication and EAP-STRAT Vol 16 are complied with. However, when a code handler's duties no longer require the control and handling of code components or as specified in this publication, the SCC/FC, or designated alternate, decertifies the individual by signing Part III of the AFGSC Form 165 and advises the individual that they are no longer a code handler (SQ/CC may advise the individuals once they have confirmed Part III of the AFGSC Form 165 has been signed).

12.3.4.1. The CRO will ensure the base COMSEC manager is notified if cryptographic access is no longer required, and SD Form 572 is completed. All access to COMSEC, code materials, and code components is terminated.

12.3.4.2. Decertification of a code handler is not required due to PCA or PCS if all prerequisite requirements identified in this publication and EAP-STRAT Vol 16 are continuously maintained. This allowance is not appropriate for circumstances extending beyond 30 calendar days.

12.3.4.3. Individuals exposed to operational coding or operational coding records will not be certified as code handlers until the observed codes are superseded.

12.3.4.4. CMR certified personnel who are exposed to operational coding or operational coding records will be decertified from code handler duties until the observed codes are superseded. **(T-0)**

12.3.4.5. An individual's certification, decertification, and codes training records may be destroyed 1 year after the individual has been decertified. **(T-0)**

12.4.1. Code handler certifying official qualification training will include the following:

12.4.1.1. SCC/FC expectation of codes certification briefing.

12.4.1.2. Knowledge demonstration / familiarity with code handler certification briefing.

12.4.2. Certifying officials will be designated in writing by the SCC/FC.

12.4. Code Controller Selection, Certification and Decertification.

12.4.1. Officer and enlisted personnel identified for selection as code controllers must meet all requirements identified in this instruction. These individuals will be proficient and knowledgeable in code handler concepts and procedures. Individuals should be identified NLT

3 months prior to PCA/PCS for manpower resource management and planned qualification requirements.

12.4.1.1. Code Handler to Code Controller Reassignment. Strict control of code control group (e.g. "X" to "A" or "X" to "B") reassignments is necessary due to the complex relationship between Worldwide Unlock Code values and code components and the split-handling of other complementary code components. For full provisions see the EAP-STRAT Vol 16.

12.4.1.2. The SCC/FC must identify the individuals' projected control group and position (e.g., B2) to ensure they have the capability to maintain the required four (4) A1, four (4) A2, four (4) B1 and four (4) B2 assigned personnel for the purpose of proper control, access, Program Verification System (PVS) key change, if needed.

12.4.2. Officer and enlisted code handlers who are selected for code controller duties will be decertified as code handlers upon assignment to OSB/576 FLTS/DOX.

12.4.3. Individuals cannot perform operational code controller tasks until they have been properly trained and certified in those tasks. Certification should not be delayed if tasks cannot be trained due to lack of equipment. Any training that cannot be accomplished due to lack of equipment should be noted on the training record and be accomplished when the equipment becomes available.

12.4.3.1. Individuals will not perform unsupervised code controller tasks until they have been certified. Before certifying a previous code controller, ensure additional considerations in EAP-STRAT Vol 16 and this instruction have been addressed. **(T-0)**

12.4.4. The SCC/FC will provide a code controller listing memorandum on the first duty day of the month to USSTRATCOM/J374, AFGSC/A3ON, and 20 AF/A3NB. This memorandum will identify current certified code controllers with DoW ID number, finalized clearance, control group and position designator (i.e., B2), certification date, and last evaluation date; projected code controllers with DoW ID number, control group, position designator, estimated certification, and evaluation date; and decertified code controllers with control group and decertification date.

12.4.4.1. Control Group Reassignment. Strict control of code control group reassignments is necessary due to the complex relationship between Worldwide Unlock Code values and code components and the split-handling of other complementary code components. For full provisions see the EAP-STRAT Vol 16. **(T-0)**

12.4.4.1.1. Control Group Change in Conjunction with Permanent Change of Station (PCS). Under most circumstances, it is not a problem to change control groups after a PCS. The split-handled launch and enable code components controlled at a previous unit by code handlers or code controllers are not complementary to similar code at the new unit. The timing of squadron code changes or Worldwide Unlock Code Change is not an issue.

12.4.4.1.1.1. If USSTRATCOM/J374 approves a control group reassignment, the individual's losing unit will forward their AFGSC or AFSPC (prior to 1 Dec 09) Form 165 to the gaining unit.

12.4.4.1.1.2. The gaining unit must coordinate to ensure compliance with all

conditions and restrictions identified by AFGSC and 20 AF/A3NB. **(T-0)**

12.4.4.1.2. Control Group Change in Conjunction with Permanent Change of Assignment (PCA). Do not recertify code controllers as code controllers of the opposite control group at the same unit. In all other cases, time control group changes for code handlers or code controllers within the same unit to strictly coincide with Worldwide Unlock Code change. **(T-0)**

12.4.5. Crypto Certification. The OSS/CC or 576 FLTS/CC will certify personnel whose duties involve the control of code components as code controllers. This certification is authorized based on coordination between the squadron commander or operations officer and the SCC/FC. A designated alternate may perform the certification recommendation at the discretion of the SCC/FC and must be noted in MFR format. Code controller certification procedures will include ICT, an initial WCPS evaluation, a briefing to the SCC/FC covering code controller concepts, duties and responsibilities, expectation for reaction to reportable situations, in addition to a personal interview with the OSS/CC or 576 FLTS/CC to ensure the provisions of EAP-STRAT Vol 16 are met. The CRO will track code controller access to USSTRATCOM CA 613202 COMSEC material. Code controller certification is documented on AFGSC Form 166. **(T-0)**

12.4.5.1. Certified Code Controller will be considered Mission Ready (MR) for WCPS coding operations duties.

12.4.6. AFGSC Form 166 (AFGSC Form 165 prior to 11 April 2017) Documentation. OSB and 576 FLTS/DOX will maintain an AFGSC Form 166 on each code controller. The form is initiated when the code controller selectee begins code controller training. Upon completion of initial training, WCPS evaluation and certification briefing, the SCC/FC signs and dates Part I of the AFGSC Form 166. When all prerequisites are completed, the code controller selectee and OSS/CC or 576 FLTS /CC sign and date Part II of the form. Once Part II is signed, the only authorized change to this form following certification will be due to a legal name change of an individual. If an administrative or clerical error is identified following signing of Part II, it will be documented utilizing a memorandum for record to be kept with the original document. For other changes (i.e., PCS/PCA with a certifying official change) a new AFGSC Form 166 will be completed re-using existing data from the original 166 at the discretion of the gaining OSB.

12.4.7. Decertification. When code controller duties no longer require the control and handling of code components, the SCC/FC, or designated alternate, decertifies the individual by signing Part III of the AFGSC Form 166 (AFGSC 165 prior to 11 April 2017) and advises the individual that they are no longer a code controller.

12.4.7.1. The CRO will ensure the local base COMSEC manager is notified that cryptographic access is no longer required and SD Form 572 is completed. All access to COMSEC, codes materials, and code components is terminated.

12.4.7.2. Decertification of a code controller is not required due to PCA or PCS if all prerequisite requirements identified in this publication and EAP-STRAT Vol 16 are continuously maintained and gaining commander accepts previous certification. This allowance is not appropriate for circumstances extending beyond 30 calendar days. **(T-0)**

12.5. Code Controller Individual Qualification Folder. Each code controller will have a six-part folder (or electronic equivalent) maintained in OSB/576 FLTS/DOX, documenting certification, position appointments, evaluation reports, and training. As a minimum the six-part folders will contain the documents identified in this publication.

Chapter 13

MISCELLANEOUS

13.1. New or Upgrade System Requirements. For new or upgraded codes portion of the ICBM weapon system, the OSB/576 FLTS/DOX training section will develop and/or review the training program to meet requirements within this instruction, AFGSCI 13-5201V1 and AFGSCI 13-5201V3.

GLENN HARRIS
Brigadier General, USAF
Director of Operations

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

DoD Directive S-5210.81, *United States Nuclear Weapons Command and Control, Safety, and Security*, April 24, 2017

CJCSI 3231.01C, *Safeguarding Nuclear Command and Control Extremely Sensitive Information*, 20 February 2019

CJCSI 3260.01F, *Joint Policy Governing Positive Control Material and Coded Control Devices*, 22 November 2019

September 2018

EAP-STRAT Volume 3, *Positive Control Policy, Procedures, and Coded Control Devices*, 01 October 2024

EAP-STRAT Volume 16, *ICBM Code Component Control Policy and Procedures*, 1 August 2025

AFPD 13-5, *Air Force Nuclear Mission*, 17 July 2018

DAFI 36-2110, *Total Force Assignments*, 2 August 2021

DAFI 36-2670, *Total Force Development*, 25 June 2020

DAFI 91-101, *Air Force Nuclear Weapons Surety Program*, 26 March 2020

DAFI 90-160, *Publications and Forms Management*, 14 April 2022

DAFI 91-204, *Safety Investigations and Reports*, 10 March 2021

DAF 91-204_AFGSCSUP, *Safety Investigations and Reports*, 5 Aug 2019

DAFMAN 17-1302-O, *Communications Security (COMSEC) Operations*, 12 Dec 2024

DoDM 5210. 42_AFMAN 13-501, *Nuclear Weapons Personnel Reliability Program (PRP)*, 23 June 2025

AFI 33-332, *Records Management and Information Governance Program*, 23 March 2020

AFH 33-337, *The Tongue and Quill*, 27 May 2015

AFI 91-114, *Safety Rules for the Intercontinental Ballistic Missile System*, 05 January 2023

AFGSCI 13-5201V1, *Rapid Execution and Combat Targeting (REACT) Crew Training and Certification*, 4 January 2022

AFGSCI 13-5201V2, *Rapid Execution and Combat Targeting (REACT) Crew Standardization and Evaluation*, 4 June 2023

AFGSCI 13-5201V3, *Rapid Execution and Combat Targeting (REACT) Crew Operations*, 4 June 2018

TCTO 21M-LGM30G-1135- ICU-II modification

TO 21M-LGM30G-12-1, *Minuteman Nuclear Surety Procedures for the WS-133A-M/B Weapon Systems*, 1 February 2022

TO 00-33B-5508, *Control and Handling of Minuteman ICBM COMSEC Material*

TO 21M-LGM30G-2-12-2, *Computer Program Loading and Command and Status System Maintenance*, 31 August 2021

TO 21M-LGM30G-2-12-4, *Missile Alert Facility Command and Control Equipment*, 11 May 2023

TO 31X8-2-2-1, *Operation Instructions, Console, Wing Code Processing System (WCPS) (P/N 10365-107-())*, 24 January 2025

TO 31X8-2-2-2, *Maintenance Instructions with Illustrated Parts Breakdown, Console, Wing Code Processing System (WCPS) (P/N 10365-107-())*, 01 November 2022

TO 31X8-2-3-1, *Operation and Maintenance Instructions with Illustrated Parts Breakdown, Console, Hardware Certification Verification Equipment (HCVE) (P/N 11800-315-11)*, 19 June 2017

Prescribed Forms

AFGSC Form 162, *576 FLTS Launch Key Record*

AFGSC Form 163, *MW Launch Key Record*

AFGSC Form 164, *Code Controller Operations Record*

AFGSC Form 165, *Code Handler Certification and Training Record*

AFGSC Form 166, *Code Controller Certification and Training Record*

Adopted Forms

AF Form 8, *Certificate of Air Crew Qualification*

AF Form 679, *Air Force Publication Compliance Item Waiver Request/Approval*

AF Form 1522, *ARMS Additional Training Accomplishment Report*

AF IMT 4329, *AF Observation, Issue or Lessons Learned (Unclassified)*

AF IMT 4329A, *AF Observation, Issue or Lessons Learned (Secret)*

AFGSC Form 91, *Record of Qualification, Certification and Associated Events*

DAF Form 847, *Recommendation for Change of Product*

SD Form 572, *Cryptographic Access Certificate (PA) (CUI)*

Abbreviations and Acronyms

AETC—Air Education Training Command

AF—Air Force

AFB—Air Force Base

AFGSC—Air Force Global Strike Command

AFH—Air Force Handbook
AFI—Air Force Instruction
AFMAN—Air Force Manual
AFMC—Air Force Material Command
AFNWC/NI—AFNWC ICBM Systems Directorate
AFNWC/NIAG—AFNWC LCC Program Branch
AFNWC/NIE—AFNWC Environment Safety and Technical Data Branch
AFNWC—Air Force Nuclear Weapons Center
AFOSH—Air Force Occupational Safety and Health
AFOTEC—Air Force Operational Test and Evaluation Center
AFSC—Air Force Specialty Code
AFSEC—Air Force Safety Center
AFSPC—Air Force Space Command
ALC—Assignment Limitation Code
ALCS—Airborne Launch Control System
ARMS—Aviation Resource Management System
BGRC—Boeing Guidance Repair Center
BMC—Basic Mission Capable
BMK—Basic Mission Knowledge
BMT—Basic Mission Training
BS/L—Bulk Storage/Loader
C4I—Command, Control, Communications, Computers, Intelligence
CA—COMSEC Account
CAP—Cryptographic Access Program
CAW—Corrective Action Worksheet
CBT—Computer Based Training
CCA—Circuit Card Assembly
CC—Commander
CCOS—Common Certification Operating System
CCSD—Cryptologic & Cyber Systems Division
CCV—Code Change Verifier
CDA—Coder-Decoder Assembly

CD—Compact Disc
CD-RW—Compact Disc Re-Writable
CHOP—Code Handler Orientation Package
CJCSI—Chairman, Joint Chief of Staff Instruction
CLS—Contractor Logistical Support
CMR—Combat Mission Ready
CMSC—Computer Memory Security Check
COG—Clarification of Guidance
COMSEC—Communications Security
CONAUTH—Controlling Authority
COP—Console Operations Program
CRE—Codes Related Event
CRO—COMSEC Responsible Officer
CRYPTO—Cryptographic
CSD(G)—Command Signals Decoder (Ground)
CSD(M)—Command Signals Decoder (Missile)
CSE—Code Storage Element
CUI—Controlled Unclassified Information
DAFC—Department of Air Force Civilian
DCS—Defense Courier Service
DMD—Data Management Device
DoD—Department of Defense
DO—Director of Operations
DoDM—Department of Defense Manual
DoW—Department of War
DTU—Data Transfer Unit
EAP—Emergency Action Procedure
ECC—Emergency Combat Capability
E-Lab—Electronics Laboratory
EMP—Electromagnetic Pulse
EMSEC—Emissions Security (formerly TEMPEST)
EMT—Electro-Mechanical Team

EPCI—Execution Plan Case Input
EPP/MA—Execution Plan Program/Message Analysis
EPP—Execution Plan Program
ESD—Electrostatic Discharge
EWO—Emergency War Order
FAM—Familiarization
FC—Flight Commander
FDD—Floppy/Flash Disk Drive
FDE—Force Development Evaluation
FD—Floppy Disk
FDM—Force Direction Message
FLTS—Flight Test Squadron
FSC—Flight Security Controller
HAF—Headquarters Air Force
HCVE—Hardware Certification Verification Equipment
HDA—Head Disk Assembly
HHQ—Higher Headquarters
HICS—Hardened Intersite Cable System
HQ—Headquarters
HSEP—Hardness Surveillance Electromagnetic Pulse (EMP) Program
IAW—In Accordance With
ICBM—Intercontinental Ballistic Missile
ICBMSG—ICBM Sustainment Group
ICBMSS—ICBM Sustainment Squadron
ICPS—ICBM Code Processing System
ICT—Initial Codes Training
ICU II—ICBM Cryptographic Upgrade-II
ID—Identification
IMT—Information Management Tool
IPB—Illustrated Parts Breakdown
IQF—Individual Qualification Folder
IST—Initial Skills Training

ITP—Individual Training Program
LAS—Launch Action Study
LCC—Launch Control Center
LCP—Launch Control Panel
LECG—Launch Enable Control Group
LEP—Launch Enable Panel
LER—Launcher Equipment Room
LF—Launch Facility
LFLCD—Launch Facility Load Compact Disk
LL—Lessons Learned
MAF—Missile Alert Facility
MAJCOM—Major Command
MCC—Missile Combat Crew
MCCM—Missile Combat Crew Member
MCU—Mechanical Code Unit
MFCC—Missile Field Control Center
MFR—Memorandum for Record
MGC—Missile Guidance Computer
MGS—Missile Guidance Set
MLP—Master Lesson Plan
MM—Minuteman
MMOC—Missile Maintenance Operations Center
MMT—Missile Maintenance Team
MQT—Missile Qualification Training
MR—Mission Ready
MSB—Missile Support Base
MSC—Missile Security Control
MW—Missile Wing
MX—Maintenance
NAF—Numbered Air Force
NC2-ESI—Nuclear Command and Control-Extremely Sensitive Information
NCOIC—Non-Commissioned Officer-In-Charge

NCO—Non-Commissioned Officer
NGAS—Northrop Grumman Aerospace Systems
NGTS—Northrop Grumman Technical Solutions
NMR—Non-Mission Ready
NSA—National Security Agency
NSCCA—Nuclear Safety Cross-Check Analysis
NSN—National Stock Number
NWSSG—Nuclear Weapons System Safety Group
OFP—Operational Flight Program
OGP—Operational Ground Program
OGV—Chief, Operations Group Standardization and Evaluation
OID—Operator Input Device
OPR—Office of Primary Responsibility
OSB—Wing Code Controller Flight
OSS—Operations Support Squadron
OST—Treaty on Open Skies
PCA—Permanent Change of Assignment
PCC—Possible Code Compromise
PCM—Positive Control Material
PC—Positive Control
PCS—Permanent Change of Station
PCTT—Possible Compromise of TDI Technology
PEN Code—Penetration Code
PEN-C—Penetration Close
PEN-D—Penetration Disclose
PEX—Patriot Excalibur
POC—Point of Contact
P-Plug—Permutation Plug
PRAP—Personnel Reliability Assessment Program
PROM—Programmable Read-Only Memory
PRP—Personnel Reliability Program
PV—Procedural Violation

PVS—Program Verification System
Q1—Qualification Level 1
Q2—Qualification Level 2
Q3—Qualification Level 3
QCO—Quality Control Observation
RCPTM—Ready Codes Program Tasking Memorandum
REACT—Rapid Execution and Combat Targeting
RIP—Ready ICBM Program
ROM—Read Only Memory
RS—Reentry System
RV—Reentry Vehicle
SAC—Strategic Air Command
SAP—SCPS Application Program
SARM—Squadron Aviation Resource Management
SAV—Staff Assistance Visit
SCC—Senior Code Controller
SCPS—SAC Code Processing System
SCSC—Squadron Code Sum Check
SELM—Simulated Electronic Launch Minuteman
SE—Shielded Enclosure
SF—Standard Form
SKL—Simple Key Loader
SME—Subject Matter Expert
SMIC—Strategic Missile Integration Center
SRAM—Static Random Access Memory
SSO—System Security Office
Stan/Eval—Standardization/Evaluation Officer
ST—Special Training
SURF—Single Unit Retrieval Format
TBA—Training Business Area
TCC—Transportation Control Center
TCI—Target Case Input

TDI—Tamper Detection Indicator
TDY—Temporary Duty
TEI—Test Execution Instruction
TEK—Traffic Encryption Key
TMP—Threat Mitigation Plan
TM—Training Manager
TOMA—Technical Order Management Authority
TO—Technical Order
TPC—Two Person Concept
TP—Training Plan
TRG—Training Group
TRS—Training Squadron
TSEC—Telecommunications Security
TTP—Tactics, Techniques and Procedures
UA—Unauthorized Access
ULS—Unauthorized Launch Studies
UL—Unauthorized Launch
UMR—Unit Master Record
UPS—Uninterruptible Power Supply
USSTRATCOM—United States Strategic Command
VCP—Voice Control Panel
VN—Verification Number
WCPS—Wing Code Processing System
WMAF—WCPS Minuteman Application Program
WSA—Weapon Storage Area
WSCE—Weapon System Control Element
WSEP—Weapons System Evaluation Program
WSP—Weapon System Processor
WSSR—Weapon System Safety Rules
WS—Weapon System
WWU—Worldwide Unlock

Office Symbols

20 AF/A3NB—20 AF/Codes Branch

509 ICBMSS/GFEA—509 ICBMSS Ground Electronics Branch

576 FLTS/DOX—576 Flight Test Squadron, Missile Systems

576 FLTS—576 Flight Test Squadron

AETC/A3TI—AETC/C4I and Training Division

AFGSC/A3ON—AFGSC/ICBM Operations Support Branch

AFGSC/IG—AFGSC/Inspector General

AFGSC/SEW—AFGSC/Weapons Safety Division

AFGSC/SEWN—AFGSC/Weapons Safety Division Nuclear Branch

DIRNSA/C62—Director, National Security Agency, Office of Nuclear Command and Control

USSTRATCOM/J374—USSTRATCOM Missile Control Branch

Attachment 2**AFGSC FORM 165/166 REVIEW CHECKLIST**

A2.1. Correctness. Are Name, Grade and Unit all correct at time of certification?

A2.2. Privacy Act. Form will have a Privacy Act statement.

A2.3. Verify. Verify code control group is correct (i. e., A or B).

A2.4. Block I.

A2.4.1. Signed by a certified Codes Trainer.

A2.4.2. Dated when the student completed “Initial Code Handler Training” on the AFGSC Form 165 or “Initial Code Controller Training” on the AFGSC Form 166, not the date the instructor signed Block I.

A2.4.3. Security Clearance Date: Must be **FINAL ADJUDICATED** clearance date.

A2.4.4. TPC/Nuclear Surety Dates: Must be less than 15 months prior to certification date.

A2.4.5. PRP Certified Date: **Must** follow after Security Date and prior to certification Date.

A2.5. Block II.

A2.6. Certification Date. The certifier’s signature date will be the latest date on the form (may be the same date as the individual being certified in same block) following all others and will be the official certification date of the code controller. This block must be signed by the individual and certifying official.

A2.7. Block III.

A2.7.1. Decertification Date: **Must** be signed by a decertifying official.

A2.8. Notes.

A2.8.1. When correcting any mistakes on form 165/166, draw a single non-obliterating line through the entry and initial.

A2.8.2. Signatures will be in **Black** or **Blue** ink only.

A2.8.3. Use System of Record to verify 165/166 hard copy. All information will match.

Attachment 3

CODE CONTROLLER INDIVIDUAL QUALIFICATIONS FOLDER REVIEW

A3.1. Code Controller Individual Qualification Folder Review. Units are encouraged to use [Table A3.1](#) to review Code Controller IQFs. The table is designed as a guide to assist units in conducting a thorough review of Code Controller IQFs similar to how SAV team members or HHQ inspectors would review them.

A3.1.1. This table does not provide a means to conduct a thorough review of supporting documentation (initials certifying all operator qualification training requirements were completed, codes group reassignment, positional appointment, etc.). Units must develop processes to ensure all prerequisites are accomplished and documented prior to applicable certifications.

Table A3.1. Code Controller Individual Qualification Folder Review.

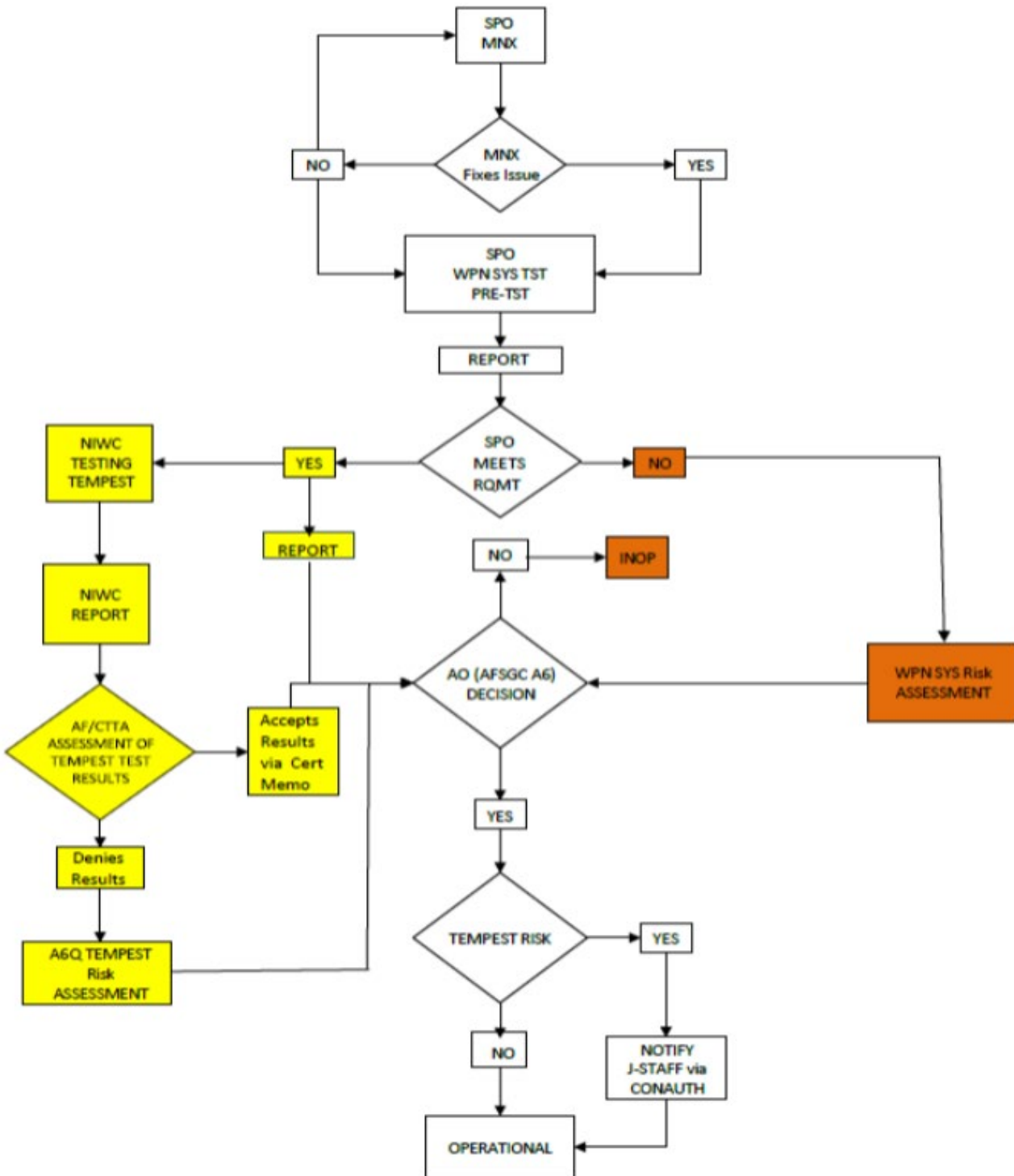
DESCRIPTION	YES	NO	N/A
Section 1 Review			
Are all documents posted in order of occurrence (newest on top)?			
Is AFGSC Form 165 Code Handler Certification and Training Record posted?			
Is AFGSC Form 165 Part III signed and dated upon assignment to OSB/576 FLTS/DOX?			
Is AFGSC Form 166 Code Controller Certification and Training Record posted?			
Is AFGSC Form 166 Part I signed by SCC/FC and dated?			
Is AFGSC 166 Part I dated same or after initial evaluation date?			
Is AFGSC Form 166 Part II signed by OSS/CC or 576 FLTS/CC?			
Section 2 Review			
Are all documents posted in order of occurrence (newest on top)?			
Is initial evaluation AF Form 8 posted (if applicable)?			
Does initial evaluation AF Form 8 identify evaluatee(s)?			
Does initial evaluation AF Form 8 identify evaluator and date of evaluation?			
Does initial evaluation AF Form 8 identify task performed and Task IDs evaluated?			
Are corrected training actions documented and completed (if required)?			
Did the Chief Training Officer provide documentation of individual training (if required)?			
Are the last two evaluation AF Form 8s or CAWs posted (if applicable)?			
Does recurring evaluation AF Form 8 or CAW identify evaluator and date of evaluation?			
Is recurring evaluation AF Form 8 or CAW within 18 months of previous evaluation?			
Does recurring evaluation AF Form 8 or CAW identify task performed and Task IDs evaluated?			

DESCRIPTION	YES	NO	N/A
Are corrected training actions documented and completed (if required)?			
Did the Chief Training Officer provide documentation of individual training (if required)?			
Is initial handler classroom training documented and dated (if required)?			
Is initial code controller classroom training documented and dated?			
Is initial code controller WCPS training documented and dated?			
Is individual training or specialty training documented (if required)?			
Section 3 Review			
Are all documents posted in order of occurrence (newest on top)?			
Is an approved memorandum for assignment group change posted (if required)?			
Is the date of the approved memorandum prior to initial code controller WCPS training date (if required)?			
Section 4 Review			
Are all documents posted in order of occurrence (newest on top)?			
Is a copy of SURF (or other proof of assignment to OSB/576 FLTS/DOX) posted?			
Is ALC "M" present on SURF (if a SURF was used)?			
Section 5 Review			
Are all documents posted in order of occurrence (newest on top)?			
Is a memorandum signed and dated by SCC/FC specifying appointment present (if applicable)?			
Is a waiver from the applicable level posted with appointment letter (if applicable)?			
Were duties officially performed in the position prior to appointment letter and/or waiver?			
Section 6 Review			
Are all documents posted in order of occurrence (newest on top)?			
Are applicable course attendance certificates or memorandum identifying course completion posted (if required)?			

Attachment 4

ICBM CODES SHIELDED ENCLOSURE REPAIR AND CERTIFICATION PROCESS

Figure A4.1. ICBM CODES SHIELDED ENCLOSURE REPAIR AND CERTIFICATION PROCESS.



Attachment 5
CODES INVENTORY TABLE

Table A5.1. Codes Inventory Table.

Inventory Frequency	Items to be Inventoried
Every 15 Days	All operationally coded LFLCDs, DTUs containing LFLCD data; launch or enable-coded equipment (LCPs, CCVs, LEPs, WCPS computers, WSP cards) (NOTES 1, 4)
Every 30 Days	All master media; encrypted CDs and disks; CTUs (if applicable); PEN D LFLCDs; DTUs containing Pen D LFLCD data, uncoded or training data coded DTUs; DMDs; KS-60s; reserve and superseded P-Plugs; Key CDs; OSB COMSEC SKLs; USWAA-61 parts A/B; USWAR-61 parts A/B; failed or damaged circuit cards; test and training code components; duplicates of operational launch switch keys. (NOTE 4)
Every 90 Days	All programs; MGS Parameters CDs; TDIs not in bulk storage; uncoded LCPs and LEPs; PROM Fuser Verifiers; CCV good and faulted ROM cards; all targeting and execution program and database media; KIV-7Ms (NOTE 4)
Semiannually	All WCPS 20-year spares. These may be inventoried in bulk. (NOTES 2, 4)
Updated UMR from USSTRATCOM/J374	Verify all materials are correctly listed and on-hand. (NOTES 3, 4)
NOTES: 1. The 576 FLTS/DOX does not conduct 15-day inventories 2. When a spares program manager changes, a physical inventory of all spares (opening and inventorying of all bulk packages) is required prior to the new spares program manager assuming responsibilities for the program. 3. The UMR inventory – a physical inventory of the listed materials or a cross-check of the listed materials against LF or LCC installation records – is accomplished by two code controllers of the appropriate control group. a. COMSEC account 613202 materials not listed on the UMR will be added to the list. Notify USSTRATCOM/J374 immediately of UMR discrepancies. (T-0)	

Inventory Frequency	Items to be Inventoried
	b. Return a signed copy of the UMR to USSTRATCOM/J374 within five working days of receipt. c. If any individual who signed the last posted UMR departs the unit, the UMR must be re-accomplished. This will release the previous individual of any accountability for the material listed on the UMR. (T-0) 4. All SCC/FC selectees will conduct a 15, 30, and 90-day inventory; an inventory of all items listed on the UMR; and a physical inventory of WCPS 20-year spares prior to assuming SCC/FC duties. a. Opening of bulk packages is not required for 20-year spares unless completed in conjunction with a program manager change. b. Items installed in the LCCs and LFs can be verified with a 100 percent audit of LCC and LF installation paperwork by the SCC/FC selectee. c. Results of these inventories will be documented and filed in OSB/576 FLTS/DOX records and with the SCC/FC appointment letter. OSBs/576 FLTS/DOX will send 20-year spares inventory reports to 20 AF/A3NB. 20 AF/A3NB will forward those reports to AFGSC/A3ON and AFNWC/NIAG.

Attachment 6**SHIELD ENCLOSURE PACE PLAN****Figure A6.1. Shield Enclosure PACE Plan.**

Shield Enclosure Primary, Alternate, Contingency, and Emergency (PACE) Plan	
Primary	Operation of WCPS with SE meeting the 100 dB attenuation requirement.
Alternate	Operation of WCPS with SE not meeting the 100 dB requirement and a signed Risk Acceptance Package (RAP)
Contingency	Lateral Coding
Emergency	Operation of WCPS with SE not meeting the 100 dB requirement and no signed