

3 APRIL 2006



Safety

**SAFETY RULES FOR
THE INTERCONTINENTAL
BALLISTIC MISSILE SYSTEMS**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ AFSC/SEWO (Maj Gilbert M. Baca)

Certified by: HQ USAF/SE
(MGen Maurice L. McFann, Jr.)

Supersedes AFI 91-114, 1 May 2003.

Pages: 21
Distribution: F

This instruction implements AFD 91-1, *Nuclear Weapons and Systems Surety*. It applies to operations with Minuteman III and Peacekeeper ICBMs and nuclear weapons dedicated for use with the missile systems. **Section A** assigns responsibilities. **Section B** contains each nuclear weapon systems' safety rules. The safety rules in **Section B** may only be changed or supplemented using procedures in AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules*. This instruction does not apply to the Air Force Reserve and Air National Guard. See **Attachment 1** for abbreviations and acronyms used in this instruction. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFMAN 37-123, (will convert to 33-363) Management of Records and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://afrims.amc.af.mil>.

SUMMARY OF REVISIONS

Changed temporary restriction to permanent rule within Air Force Instruction. Removed reference to interflight connection and checkout procedures. Changed USCAL 193 to USWAC 4900. Provided exception to removing re-entry system on WS-133 for missile guidance set or propulsion system maintenance. Changed name from Logistics Group to Maintenance Group Commander for approval for maintenance before sunrise and after dark. Removed reference to commanding an infinite time delay during simulated electronic launch for Minuteman III. Added procedures for an anomaly during simulated electronic launch for Peacekeeper.

Section A—Authority, Limitations, and Responsibilities	3
1. Secretary of Defense (SecDef) Direction.	3
2. Temporary Limitations.	3
3. Functional Responsibilities.	3

Section B—Safety Rules 3

4. General Guidance. 3

5. Specific Guidance. 4

6. Security and Control Criteria. 4

7. Tamper Control and Detection. 6

8. Handling and Storage of Critical Components and Certified Software. 7

9. Operational Code Control. 7

10. Personnel Reliability. 8

11. Troubleshooting, Modifications and Use of Procedures, and Checklists. 8

12. Warhead Storage. 8

13. Nuclear Identification. 8

14. Logistics Movement of Nuclear Weapons by Cargo Aircraft. 9

15. Operations Involving an Assembled Weapon System. 9

16. Operations Involving Maintenance on an Assembled Weapon System 11

17. Single Launch Control Center Operations. 12

18. Emergency Combat Capability Operations 12

19. Simulated Electronic Launch-Minuteman (SELM) Tests 12

20. Simulated Electronic Launch--Peacekeeper (SELP) Tests: 14

21. Unique Signal Device Assembly (USDA) Connectivity Test. 17

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 18

Section A—Authority, Limitations, and Responsibilities

- 1. Secretary of Defense (SecDef) Direction.** The SecDef Directs the Secretary of the Air Force to implement the rules.
- 2. Temporary Limitations.** The Air Force may impose restrictions on application of safety rules.
- 3. Functional Responsibilities.**
 - 3.1. The Commander, Air Force Safety Center:
 - 3.1.1. Ensures that the safety rules work, providing maximum safety consistent with operational requirements.
 - 3.1.2. Ensures that units follow the safety rules.
 - 3.2. Using Major Commands (MAJCOM):
 - 3.2.1. Ensure that their units follow the safety rules.
 - 3.2.2. Ensure that all safety standards and procedures agree with the approved safety rules.
 - 3.2.3. Inspect for compliance.
 - 3.3. Air Force Materiel Command (AFMC) ensures that its manuals, checklists, and technical orders do not conflict with the safety rules.

Section B—Safety Rules

- 4. General Guidance.** Per DoD 3150.2M, *DoD Nuclear Weapon System Safety Program Manual*, general safety rules apply to all nuclear weapons and nuclear weapon systems. General safety rules primarily apply safety policy and shall be included as part of the Air Force's safety rules package.
 - 4.1. Safety rules always apply, even during war.
 - 4.1.1. Nuclear weapons shall not be intentionally exposed to abnormal environments except in an emergency.
 - 4.1.2. Nuclear weapons shall not be used to training or for troubleshooting (i.e., to confirm the existence of a fault, aid in fault isolation, or verify that a fault has been corrected except as explicitly allowed by a specific safety rule).
 - 4.1.3. Nuclear weapons may be used for exercises except when explicitly prohibited by specific safety rules.
 - 4.1.4. Only certified procedures, personnel, equipment, facilities, and organizations, authorized by the appropriate level of authority, shall be employed to conduct nuclear weapon system operations.
 - 4.1.5. The total number of personnel performing nuclear weapon system operations shall be held to the minimum consistent with the operations performed.
 - 4.1.6. At least two authorized persons, who meet the requirements of the Two-Person Concept as defined in AFI 91-101, must be present during any operation with a nuclear weapon, except when authorized by a specific safety rule, i.e. alert fly. They must be able to detect incorrect or unautho-

alized procedures in the task being performed. They must also have knowledge of and understand applicable safety and security requirements.

4.1.7. Personnel that have physical access to nuclear weapons must be qualified under the PRP, in accordance with DoD Directive 5210.42.

4.1.8. Physical security will be maintained, in accordance with DoD Directive 5210.41.

4.1.9. Nuclear weapons will be transported as determined by the Combatant Commander or the Military Department, in accordance with DoD Directive 4540.5. Additionally, the following safety guidance applies:

4.1.9.1. Movement(s) will be kept to a minimum consistent with operational requirements.

4.1.9.2. Custody and accountability transfers during logistic movements shall be by courier receipt system to ensure positive control.

4.1.10. Permissive action link (PAL) operations shall be, in accordance with plans and procedures prescribed by the applicable combatant command and technical publications. (N/A ICBM because PAL is not part of weapon system)

4.1.11. Verification that a nuclear warhead is not present in a test assembly must be made utilizing nonnuclear assurance procedures at the last practical opportunity agreed upon by the Department of Defense and/or DOE before the conduct of an operational test.

4.1.12. Deviations from safety rules are permitted in an emergency, except as follows:

4.1.12.1. U.S. custody must be maintained until receipt of a valid nuclear control order that permits transferring U.S. nuclear weapons to non-U.S. delivery forces. (N/A ICBM because there are no non-U.S. delivery forces)

4.1.12.2. Nuclear weapons shall not be expended unless a valid, properly authenticated nuclear control order conveying release or expenditure authority is received.

4.1.12.3. Jettisoning of nuclear weapons is permitted in the event of an emergency, and is to be accomplished according to plans and procedures prescribed for the area of operations. (N/A ICBM because there is no jettison capability)

NOTE: DoD Directive 3150.2, *DoD Nuclear Weapon Systems Safety Program*, December 23, 1996, defines an emergency as an “unexpected occurrence or set of circumstances in which personnel or equipment unavailability, due to accident, natural event, or combat, may demand immediate action that may require extraordinary measures to protect, handle, service, transport, jettison, or employ a nuclear weapon.”

5. Specific Guidance.

5.1. These safety rules, weapon system features, operational and administrative controls, and technical procedures ensure that the ICBM weapon system meets nuclear weapon system safety standards in AFI 91-101, *Air Force Nuclear Weapons Surety Program*.

5.2. Violations of referenced instructions do not constitute WSSR violations unless specifically identified in this document.

6. Security and Control Criteria.

- 6.1. DoD C-5210.41-M, *Nuclear Weapon Security Manual (U)*, and Air Force Supplement, apply.
- 6.2. A Security Forces Two-Person Concept team must continuously guard a launch facility (LF) with a reentry system (RS) present if any of the following conditions exist:
 - 6.2.1. LF status cannot be monitored (LF Status Out or LF Down).
 - 6.2.2. The B circuit combination has been compromised.
 - 6.2.3. The secondary vault door cannot be fully raised and secured.
 - 6.2.4. The launcher closure is not locked in the closed position.
 - 6.2.5. Inner zone and outer zone security systems are not reporting true status.
 - 6.2.6. An LF is not cryptographically authenticating (LF not authenticated (LFNA) indication received).
- 6.3. A Two-Person Concept team must continuously guard an LF without an RS present, which contains operationally certified critical components, if any of the following conditions exist:
 - 6.3.1. LF status cannot be monitored (LF Status Out or LF Down).
 - 6.3.2. The B circuit combination has been compromised.
 - 6.3.3. The secondary vault door cannot be fully raised and secured.
 - 6.3.4. The launcher closure is not locked in the closed position.
 - 6.3.5. Inner zone and outer zone security systems are not reporting true status.
 - 6.3.6. An LF is not cryptographically authenticating (LF not authenticated (LFNA) indication received).
- 6.4. Two Security Forces individuals qualified under the Two-Person Concept, one of whom may be in rest status on site, must continuously guard an LF with an RS present, if any of the following conditions exist:
 - 6.4.1. The A circuit combination has been compromised.
 - 6.4.2. The A circuit vault cannot be secured.
 - 6.4.3. The inner zone security system (IZ) is not reporting true status, if outer zone security system (OZ) is functional.
 - 6.4.4. The OZ security system is not reporting true status, if IZ is functional.
- 6.5. Two individuals qualified under the Two-Person Concept, one of whom may be in rest status on site, must continuously guard an LF without an RS present, that contains operationally certified critical components, if any of the following conditions exist:
 - 6.5.1. The A circuit combination has been compromised.
 - 6.5.2. The A circuit vault cannot be secured.
 - 6.5.3. The IZ security system is not reporting true status. (OZ Functional)
 - 6.5.4. The OZ security system is not reporting true status. (IZ Functional)

7. Tamper Control and Detection. AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs*, applies.

- 7.1. Controls must prevent unauthorized seal use and handling.
- 7.2. A Two-Person Concept team must install the seals.
- 7.3. A Two-Person Concept team must inspect the seals on the following components at each crew changeover.
 - 7.3.1. Launch control panel (LCP).
 - 7.3.2. Launch enable panel (LEP).
 - 7.3.3. Coder-Decoder-Indicator drawer (WS-118 only).
 - 7.3.4. Secure data unit (SDU) keying variable door (WS-118 only).
 - 7.3.5. Launch enable control group signal panel (LECGSP) (WS-118 only).
 - 7.3.6. WSC computer processor-verifier drawer (WS-118 only).
 - 7.3.7. Message processing auxiliary storage device (WS-118 only).
 - 7.3.8. Spare drawer (URD 16231A5) (WS-118 only).
 - 7.3.9. WSC plated wire memory unit drawer (WS-118 only).
 - 7.3.10. Memory controller group (MCG) controller-synchronizer drawer (WS-118 only).
 - 7.3.11. MCG magnetic drum memory unit drawer (WS-118 only).
 - 7.3.12. Coder-decoder assembly (CDA) drawer (WS-133 only).
 - 7.3.13. CDA secure data unit door. (WS-133 only).
 - 7.3.14. Weapon system processor (WSP) drawer (WS-133 only).
 - 7.3.15. Diagnostic port access panel (WS-133 only).
 - 7.3.16. Diagnostic port access door (WS-133 only).
 - 7.3.17. Right voice control panel (WS-133 only).
 - 7.3.18. Console power control and distribution unit (WS-133 only).
 - 7.3.19. Rapid message processor (WS-133 only).
 - 7.3.20. Additionally, one operationally coded LCP, LEP, LECGSP, and SDU keying variable temporarily stored in the LCC (n/a during emergency combat capability operations) for which the equipment is intended when:
 - 7.3.20.1. Squadron code change is in process.
 - 7.3.20.2. Reposturing is in process, after simulated electronic launch testing or category B operations.

NOTE: In these instances, seal the carrying case that stores the item with at least one seal on each of the case's sides adjacent to the hinged side.

- 7.4. If the integrity of all seals on the above components is lost or in doubt:

7.4.1. Maintain continuous Two-Person Concept control of the protected item until the seal integrity is restored or replaced.

7.4.2. Investigate according to AFI 91-204, *Safety Investigations and Reports*.

8. Handling and Storage of Critical Components and Certified Software. AFI 91-105, *Critical Components*, applies.

9. Operational Code Control.

9.1. Do not let an individual, a code courier team, or an installation team handle, have access to, or have any combination of codes or encoder or decoder devices, at the same time, that reveal the information needed to launch a nuclear weapon. A Two-Person Concept team must control any device containing operational code data until the data is overwritten, superseded, or destroyed.

9.2. Deny LF entry to an individual who had access to a computer memory security check (CMSC) number that the wing code processing system (WCPS) calculated for that LF until the LF's missile guidance computer calculates the CMSC number and the number is verified.

9.3. Deny launch control center (LCC) entry to an individual who had access to a computer memory confidence check (CMCC) number that the WCPS calculated for that LCC until the weapon system controller (WSC) at that LCC calculates the CMCC number and the number is verified. (WS-118 only)

9.4. Before using a squadron's data set to prepare operational code materials for the assembled weapon system, ensure the unit WCPS computer verifies the squadron code sum check (SCSC) and G-code sum check numbers that the USSTRATCOM code processing system (SCPS) computer calculated.

9.5. Ensure proper escort for an individual who seeks entry to an LCC or LF containing operational codes if the individual has had access to:

9.5.1. The current operational code values, or

9.5.2. The SCPS or WCPS during preparation of current operational code data.

9.6. Do not store USWAC 401 or USWAC 4900 documents in an LCC.

9.7. Make sure these LCC items, if installed, have at least one independently numbered seal, of a type that AFI 91-104 identifies:

9.7.1. Launch control panel (LCP).

9.7.2. Launch enable panel (LEP).

9.7.3. Coder-decoder-indicator drawer (WS-118 only).

9.7.4. Secure data unit (SDU) keying variable door (WS-118 only).

9.7.5. Launch enable control group signal panel (LECGSP) (WS-118 only).

9.7.6. WSC computer processor-verifier drawer (WS-118 only).

9.7.7. Message processing auxiliary storage device (WS-118 only).

9.7.8. Spare drawer (URD 16231A5) (WS-118 only).

- 9.7.9. WSC plated wire memory unit drawer (WS-118 only).
- 9.7.10. Memory controller group (MCG) controller-synchronizer drawer (WS-118 only).
- 9.7.11. MCG magnetic drum memory unit drawer (WS-118 only).
- 9.7.12. Coder-decoder assembly (CDA) drawer (WS-133 only).
- 9.7.13. CDA secure data unit door. (WS-133 only).
- 9.7.14. Weapon system processor (WSP) drawer (WS-133 only).
- 9.7.15. Diagnostic port access panel (WS-133 only).
- 9.7.16. Diagnostic port access door (WS-133 only).
- 9.7.17. Right voice control panel (WS-133 only).
- 9.7.18. Console power control and distribution unit (WS-133 only).
- 9.7.19. Rapid message processor (WS-133 only).

9.8. In addition to installed LCC equipment, one operationally coded LCP, LEP, LECGSP, and SDU keying variable may be temporarily stored in the LCC (n/a during emergency combat capability operations) for which the equipment is intended when :

- 9.8.1. Squadron code change is in process.
- 9.8.2. Reposturing is in process, after simulated electronic launch testing or category B operations.

NOTE: In these instances, seal the carrying case that stores the item with at least one seal on each of the case's sides adjacent to the hinged side. (Paragraph 7. describes other requirements.)

- 9.9. Code the secure code device only inside the WCPS shielded enclosure. (WS-118 only)
- 9.10. Do not use the magnetic tape unit to load operational weapon system controller Pen C codes in the launch control center. (WS-118 only)

10. Personnel Reliability. AFI 36-2104, *Nuclear Weapons Personnel Reliability Program*, and DoDD 5210.42, *Nuclear Weapon Personnel Reliability Program*, apply.

11. Troubleshooting, Modifications and Use of Procedures, and Checklists.

- 11.1. Do not use nuclear weapons to troubleshoot equipment faults.
- 11.2. Use only equipment, procedures, or checklists that are consistent with US Air Force-approved publications for any operation directly associated with nuclear weapons or nuclear weapon systems.
- 11.3. The MAJCOM must approve all ICBM publications and modifications and these publications and modifications must conform to the safety rules and the DoD Nuclear Weapon System Safety Standards.

12. Warhead Storage. Secure in DoD-approved facilities.

13. Nuclear Identification. Set up administrative controls and procedures to provide positive means of distinguishing between:

13.1. Nuclear warheads and training shapes.

13.2. Containers (including shipping and storage containers, RSs, and reentry vehicles (RVs)) with nuclear warheads and containers without nuclear warheads.

14. Logistics Movement of Nuclear Weapons by Cargo Aircraft. AFI 91-115, *Safety Rules for Nuclear Logistics Transport by Prime Nuclear Airlift Force*, applies.

15. Operations Involving an Assembled Weapon System. These rules apply when an RS containing a nuclear warhead is mated to a missile:

15.1. Except during emergency combat capability (ECC) operations or simulated electronic launch tests, at least two LCCs in a squadron must monitor the status of, and be able to inhibit, each operational LF in the squadron. If only one LCC can monitor and inhibit, crews must begin single LCC operations or have affected LF's safed in accordance with following paragraph.

15.2. If any of the conditions in subparagraphs **15.2.1.** through **15.2.4.** exist, manually lock the affected LF's Safety Control Switch (SCS) in the SAFE position or (for WS-133 only) install the missile safing pins until Emergency action procedures (EAP) direct return to a normal configuration:

15.2.1. An LCC can insert a launch command, the LF can process the command, and no other LCC can inhibit and monitor the LF.

15.2.2. No LCC can prevent Airborne Launch Control System (ALCS) aircraft access (the ability to insert enable or launch commands), and ALCS access is not authorized.

15.2.3. A missile cannot respond to an inhibit launch command and the missile is not in:

15.2.3.1. The standby NO-GO mode or LF NO-GO mode (WS-133A-M).

15.2.3.2. The standby NO-GO mode or the auxiliary status generator (ASG) mode (WS-133B).

15.2.3.3. Critical NO-GO mode or missile shutdown mode (WS-118).

15.2.4. LF status cannot be monitored (LF Status Out or LF Down) unless one of these states occurred first:

15.2.4.1. The LF NO-GO mode (WS-133A-M).

15.2.4.2. The ASG mode (WS-133B).

15.2.4.3. Critical NO-GO mode (WS-118).

15.3. These crewmember procedures apply in the LCC:

15.3.1. The Missile Combat Crew Commander and the Deputy Missile Combat Crew Commander must be on duty at the same time.

15.3.2. One crewmember at a time may sleep on duty, but both must be awake and capable of detecting an unauthorized act if:

15.3.2.1. The sealed authenticator container is unlocked and authenticators are present.

15.3.2.2. Translate code values are installed.

15.3.2.3. A possible or confirmed code compromise affects the LCC, flight area, or squadron.

- 15.3.2.4. The integrity of all seals on an installed component identified in paragraph 9.7. and 9.8. is lost or in doubt.
- 15.3.2.5. The LCC blast door is not secured by at least one of the following methods:
 - 15.3.2.5.1. Blast door pins extended
 - 15.3.2.5.2. Blast door latch engaged
- 15.3.2.6. The LCC is operating in a single LCC configuration.
- 15.3.2.7. Someone other than the crew is in the LCC. *EXCEPTIONS:* The wing commander, vice commander, operations group commander, deputy operations group commander, or the commander of the squadron to which the LCC belongs when the non-crewmember:
 - 15.3.2.7.1. Has had no access to either the Minuteman or Peacekeeper unauthorized launch or launch action studies.
 - 15.3.2.7.2. Knows no portion of the current worldwide unlock values or secure selective unlock values.
 - 15.3.2.7.3. Has current Personnel Reliability Program certification.
 - 15.3.2.7.4. Is the squadron's only visitor.
- 15.3.3. Both crewmembers must authenticate an execution order before initiating an enable or execute launch command.
- 15.3.4. When in receipt of unauthorized enable or execute launch command indications the crew must immediately begin:
 - 15.3.4.1. Inhibit procedures. (WS-133B)
 - 15.3.4.2. Inhibit/anti-jam procedures. (WS-133A-M or WS-118)
- 15.3.5. Unless in receipt of any authenticated execution message, crews must immediately accomplish LF status out procedures when uncoordinated LF status out indications exceed 1 minute and occur in modes other than the anti-jam transmission mode. (WS-118 only)
- 15.3.6. Initiate the remote data change halt command immediately after receiving indications of unauthorized sole-survivor retargeting actions.
- 15.4. Keep these LCC switches as listed until an authenticated execution order directs otherwise:
 - 15.4.1. Enable switch in the SET position.
 - 15.4.2. Launch switch in the SET position (WS-133A-M and WS-118).
 - 15.4.3. Launch switch in the off position (WS-133B).
- 15.5. Do not allow ALCS access to LFs until EAP authorize access.
- 15.6. Do not allow the Airborne Launch Control Center (ALCC) hold-off timer to reach zero until authorized by EAP.
- 15.7. Cooperative Enable Timers: (WS-133 only)
 - 15.7.1. Maximum setting for display timer is 1 second.
 - 15.7.2. Maximum setting for entry timer is 4 seconds.

15.8. In order to provide sufficient time for monitoring LCCs to recognize and inhibit a single execute launch command the minimum time for the one-vote timer will be:

15.8.1. 30 minutes for WS-133A-M and WS-118.

15.8.2. 6 hours for WS-133B.

16. Operations Involving Maintenance on an Assembled Weapon System :

16.1. As soon as possible after personnel enter the launcher, manually safe the LF's SCS and remove the SCS key from the lock pin assembly. The SCS must stay in the SAFE position when personnel occupy the launcher, except when the only maintenance being done is observing the SCS during SCS tests.

16.2. Pin all safe and arm devices and arm/disarm devices in the SAFE position before: (WS-133)

16.2.1. Removing the SCS lockpin during maintenance (except as noted above for SCS tests).

16.2.2. D-Box maintenance.

16.2.3. Personnel enter the launch tube to:

16.2.3.1. Connect, disconnect, or troubleshoot the upper or lower umbilical.

16.2.3.2. Weld.

16.2.3.3. Remove or replace the RS.

16.2.3.4. Remove, replace, or perform maintenance on the:

16.2.3.4.1. Missile.

16.2.3.4.2. Missile guidance set or propulsion system rocket engine.

16.3. Remove the RS from the missile for:

16.3.1. Missile recycle.

16.3.2. RS or warhead maintenance.

16.3.3. Missile guidance set or propulsion system maintenance (WS-133), except as authorized by AFSC/SEW.

16.3.4. Requirements identified in technical order 21-LG118A-12 (WS-118) and 21M-LGM30F-12 (WS-133).

16.4. Do not install a RS on the missile until an operational code has been inserted into the command signal decoder (Missile) (CSD (M)) and valid verification number (VN) has been obtained and matches the VN computed by the WCPS. For downstages with an error in the reverify mode, procedures in the 2-1 series technical order may be used in lieu of a verification number. Do not remove the operational code in the CSD (M) until the RS has been removed from the missile or mechanically and electrically isolated via a SELM test wafer. (WS-133 only)

16.5. Maintenance after dark is not prohibited. However, maintenance requiring a penetrated LF, occurring after official sunset or before official sunrise must be approved by the Maintenance Group Commander or higher.

17. Single Launch Control Center Operations.

17.1. The installed LCP must be coded only with the operational inhibit code. Dissipate all operational launch code data from mechanical code units (MCU). *EXCEPTION:* During predetermined advanced readiness conditions, as specified by EAP or higher headquarters directives, missile combat crews (MCCs) need not dissipate operational codes in the single LCC. However, begin ECC operations according to paragraph 18. as soon as the situation permits.

17.2. Keep all operational LCPs for the affected squadron under Two-Person Concept control or in a secured area requiring Two-Person Concept team access. Keep these LCPs at the missile support base until predetermined levels of advanced readiness when EAP or higher headquarters directives authorize delivery to the LCC to support ECC operations.

17.3. A fully programmed spare WSC or head disk assembly (HDA) must be available in case of failure.

17.4. The LCC requires continuous Two-Person Concept control (paragraph 15.3.2.6.).

18. Emergency Combat Capability Operations : During ECC operations, the rules in paragraphs 4. through 16. apply, except those in paragraphs 9.8. and 15.1. These rules also apply:

18.1. Operational LCPs may be taken to, and stored in, the LCC.

18.2. When operational LCPs are present, two MCCs (four crewmembers in all) must have concurrent duty within the LCC. At least two crewmembers must be awake at all times.

18.3. The installed LCP must be coded only with the operational inhibit code. LCPs with operationally coded, launch code MCUs may be installed at predetermined levels of advanced readiness as directed by higher headquarters or EAP.

18.4. Both MCCs must authenticate an execution order before initiating an enable or an execute launch command.

18.5. A fully programmed spare WSC (WS-118) or HDA (WS-133) must be available in case of failure.

19. Simulated Electronic Launch-Minuteman (SELM) Tests : During SELM tests, the rules in paragraph 4. though 16. apply, except those in paragraph 15.1. These rules also apply:

19.1. RS Removal. Remove the RS from the test LF(s) when:

19.1.1. Any ordnance item will be expended.

19.1.2. Only one LCC is used in the test configuration.

19.1.3. An anomaly occurs that is nuclear safety related or increases the possibility of an abnormal environment occurring.

19.2. Isolation Procedures.

19.2.1. For the WS-133A-M, cable interconnectivity between operational flights must be such that a single fault will not result in single LCC control of an operational flight or LF(s).

19.2.2. For the WS-133B, nontest LFs not under the cable control of two nontest LCCs must be interrogated in at least two MF radio timeslots.

19.2.3. Electrically disconnect test LFs and test LCCs from the nontest LFs and LCCs on the command circuits of the hardened intersite cable network:

19.2.3.1. Isolate WS-133A-M LCC command lines by removing the corresponding connecting links in the LF interconnecting box and installing command-line isolators.

19.2.3.2. Isolate WS-133B command lines by installing command-line isolators. Change the operating frequency in the test LFs and test LCCs to maintain medium frequency (MF) radio isolation.

19.2.4. Maintain operational status interrogation routines in cable and (WS-133B) radio modes in the nontest portion of the test squadron.

19.2.5. Verify inhibit command isolation immediately before airborne and ground tests.

19.3. Codes.

19.3.1. Administrative controls and procedures must positively distinguish code tapes and devices containing test codes from those with operational codes.

19.3.2. Operational SDU keying variables must be used during SELM tests. Replace all other operational codes at test LFs and test LCCs with test codes before SELM testing.

19.3.3. Install test-coded LCPs in the test LCCs before the last-look inspection.

19.3.4. For SELM tests involving ALCS use excluded test "X," "Y," and "L" code blocks to generate codes installed in test LFs and test LCCs.

19.4. Commands.

19.4.1. After the test ALCS aircraft issues the first enable command, determine the status of each LF (of the same weapon system) in the MAJCOM. After verifying the nontest LFs did not process the enable command, the ALCS aircraft must transmit the inhibit launch command and poll the test squadron to ensure that no nontest facility received the inhibit launch command.

19.4.2. If nontest facilities in the MAJCOM respond to test commands, proceed only after determining cause and completing necessary corrective actions.

19.5. Safing Actions.

19.5.1. Missile safing pins will be installed in all test LFs from SELM posture until EWO reposition.

19.5.2. During the ground test, manually safe any nontest LF in the same squadron for which status monitoring is lost.

19.5.3. Before or during the ALCS test, if status monitoring is lost for any nontest LF in the same wing, manually safe that LF. Stop the test until safing is completed. This safing requirement applies only to like configurations in wings with multiple system configurations.

19.6. Airborne Launch Control System.

19.6.1. Make sure the test ALCS aircraft transmits only proper commands by verifying:

19.6.1.1. The coded portable storage unit and volatile keying assemblies (VKA) on board the test ALCS aircraft contain only test data.

19.6.1.2. All commands transmitted from the ALCS aircraft to the test LFs are on the frequencies and tones designated for the SELM tests.

19.7. Status Monitoring.

19.7.1. For test LFs with an RS, two LCCs in the test squadron must monitor the status of, and be able to inhibit, each such test-configured LF. If less than two LCCs retain the ability to monitor or inhibit, stop the test until the condition is corrected.

19.7.2. For nontest LFs at least two nontest LCCs in the test squadron must be operational and capable of monitoring and transmitting the inhibit launch command to nontest LFs. If less than two nontest LCCs retain their monitoring or inhibiting capabilities, stop the test. The remaining nontest LCC must begin single LCC operations. (paragraph 17.).

19.7.3. Do not start testing again until the proper number of LCCs are available to control test and nontest LFs.

19.8. Last-Look Inspection. Before testing, a Two-Person Concept team composed of individuals who were not on the maintenance team that configured the test LF must conduct a last-look inspection.

19.8.1. The last-look inspection must verify that personnel:

19.8.1.1. Disconnected the first-stage ignition branch of the lower umbilical cable from the D-Box and capped the branch.

19.8.1.2. Properly pinned all safe and arm devices and arm/disarm devices, and disconnected and capped the RS cable.

19.8.1.3. Configured the test LF(s) properly.

19.8.1.4. Removed the missile guidance set battery from the missile.

19.8.1.5. Installed all command-line isolators properly.

19.8.2. The last look inspection must be performed again if the launch tube is subsequently penetrated.

19.8.3. The following procedures must be performed again if only the LER is entered after the last-look inspection to verify that personnel:

19.8.3.1. Configured the test LF(s) properly.

19.8.3.2. Removed the missile guidance set battery from the missile.

19.8.3.3. Installed all command-line isolators properly.

20. Simulated Electronic Launch--Peacekeeper (SELP) Tests: During SELP tests, the rules in paragraph 4. through 16. apply, except those in paragraph 15.1. These rules also apply:

20.1. RS Removal. Remove the RS from the test LF if:

20.1.1. Any ordnance item will be expended.

20.1.2. Only one LCC is used in the test configuration.

20.1.3. An anomaly occurs that is nuclear safety related or increases the possibility of an abnormal environment occurring.

20.2. Isolation Procedures.

20.2.1. Install test-coded LCPs in each test LCC before missile startup of any test-configured missile.

20.2.2. Conduct an inhibit test of both test and nontest LFs using the test-coded LCPs before last-line cable isolation to verify code isolation.

20.2.3. Electrically disconnect test LFs and LCCs from nontest LFs and LCCs on the command circuits of the hardened intersite cable network.

20.2.4. Isolate command lines by removing the corresponding connecting links in the test LF and LCC interconnecting boxes and installing command-line isolators at test LFs.

20.2.5. Verify isolation immediately before airborne and ground tests.

20.3. Codes.

20.3.1. Use operational SDU keying variables, secure code device (SCD) "L" Codes, and KI-45 mode B keying variables during SELP tests.

20.3.2. For SELP tests not involving ALCS use test "X," "Y," "L," and "G" code blocks and test keying variable plug with associated test "F" data to generate codes installed in test LFs, LCCs.

20.3.3. For SELP tests involving ALCS use excluded test "X," "Y," and "L" code blocks and test "G" code data and variable plugs with associated test "F" data to generate codes installed in test LF, LCC, and ALCS Aircraft.

20.3.4. Use SELP-dedicated operational KI-45 mode A keying variables in ALCS aircraft.

20.3.5. Replace operational SCDs at test LF, with newly coded operational SCDs after the SELP test.

20.3.6. Set up administrative controls and procedures to positively distinguish code tapes and devices with operational codes from those with test and SELP codes.

20.4. Commands.

20.4.1. Before issuing the enable, execute launch command, and automatic launch command (AUTO) commands, verify infinite time delay status of each nontest LF in the squadron or manually safe the LF before continuing the test.

20.4.2. For ALCS tests, verify radio mode (RADMO) status is not reporting for any nontest LF in the test squadron before transmitting Airborne Launch Control Center commands or manually safe the LF before continuing the test.

20.4.3. If nontest facilities (of the same weapon system) accept test commands, proceed only after determining cause and completing corrective action.

20.5. Manual Safing.

20.5.1. The test LF(s) must stay manually safed until the last-look inspection, except during remote missile test.

20.5.2. Before or during the SELP test, if status monitoring is lost for any nontest LF, if LF status is reported by auxiliary status reply, or if RADMO status is reported, stop the test until that nontest LF is manually safed.

20.6. Airborne Launch Control System.

20.6.1. Make sure the ALCS test aircraft transmits only proper commands by verifying that SELP-dedicated operational Portable Storage Unit and volatile keying assemblies on board the ALCS test aircraft contain only test and SELP data.

20.6.2. After the ALCS test aircraft transmits the first enable command, determine the status of each test and nontest LF (of the same weapon system). After verifying that the test LFs accepted the enable command and nontest LFs did not, the ALCS test aircraft must transmit the inhibit command. Check test LF status to verify that the LF accepted the inhibit command and returned to the disabled state. Do this command sequence before the ALCS test aircraft transmits the first AUTO command to verify appropriate ALCS test and SELP codes.

20.7. Status Monitoring.

20.7.1. Two test LCCs must monitor the status of, and be able to inhibit each test LF with an RS. If either LCC loses monitoring capability, immediately guard all affected LFs until the condition is corrected.

20.7.2. At least two nontest LCCs must monitor the status of, and be able to inhibit, each nontest LF. If not, the crews must assume single LCC operations (paragraph 17.).

20.7.3. Do not start testing again until the proper number of LCCs are available to control test and nontest LFs.

20.8. Last Look Inspections.

20.8.1. A Two-Person Concept team composed of individuals who were not on the maintenance team that configured the test LF(s) must conduct the last-look inspection.

20.8.2. Before test execution, the Two-Person Concept team conducting the last-look inspection must verify that personnel have:

20.8.2.1. Disconnected cable W8252 from the D-Box and connected it to the W02, which connects to the Data Acquisition System.

20.8.2.2. Put the unique signal device assembly (USDA) in the "SAFE" position by temporarily reconnecting cable W8260 to the D-Box and verifying the missile operational status reply (MOSR) 59 resets.

20.8.2.3. Disconnected and capped the USDA drive cable W8260.

20.8.2.4. Connected the SELP cable W10 to stage four cables W4MP3 and W4HP2.

20.8.2.5. Configured ordnance items properly. (The team must verify appropriate status of GMR 23 and MOSRs 12 and 13 with the controlling LCC.).

20.8.2.6. Installed all command-line isolators properly.

20.8.3. If someone enters the launcher equipment room after these inspections, perform the procedures in paragraph 20.8.2. again.

21. Unique Signal Device Assembly (USDA) Connectivity Test. In addition to the rules in paragraph 4. through 19. the following rules apply:

21.1. Remove the RS from the test missile prior to the test.

21.2. Before reinstalling the RS, load the operational launch control program and verify the USDA is in the "SAFE" position.

MAURICE L. MCFANN, JR., Major General
Chief of Safety

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****Abbreviations and Acronyms***

AFMC—Air Force Materiel Command
ALCC—Airborne Launch Control Center
ALCS—Airborne Launch Control System
ASG—Auxiliary Status Generator
AUTO—Automatic Launch Command
CDA—Coder-Decoder Assembly
CDB—Command Data Buffer
CMCC—Computer Memory Confidence Check
CMSC—Computer Memory Security Check
D-BOX—Distribution Box
DoD—Department of Defense
DOE—Department of Energy
DOJ—Department of Justice
EAP—Emergency Action Procedures
ECC—Emergency Combat Capability
EP—Enable Panel
EWO—Emergency War Orders
GMR—Ground Maintenance Response
HDA—Head Disk Assembly
ICBM—Intercontinental Ballistic Missile
ICPS—ICBM Code Processing System
JCS—Joint Chiefs of Staff
JS—Joint Staff
LCC—Launch Control Center
LCP—Launch Control Panel
LECGSP—Launch Enable Control Group Signal Panel
LF—Launch Facility
LFNA—Launch Facility Not Authenticated
MAJCOM—Major Command

MCC—Missile Combat Crew
MCG—Memory Controller Group
MCU—Mechanical Code Unit
MF—Medium Frequency
MK—Mark
MOSR—Missile Operational Status Reply
RADMO—Radio Mode
REACT—Rapid Execution and Combat Targeting
RS—Reentry System
RV—Reentry Vehicle
SCD—Secure Code Device
SCS—Safety Control Switch
SCSC—Squadron Code Sumcheck
SDU—Secure Data Unit
SECDEF—Secretary of Defense
SELM—Simulated Electronic Launch--*Minuteman*
SELP—Simulated Electronic Launch--*Peacekeeper*
URD—Unit Reference Designator
USDA—Unique Signal Device Assembly
VKA—Volatile Keying Assembly
WCPS—Wing Code Processing System
WSC—Weapon System Controller
WSP—Weapon System Processor

DISTRIBUTION

HQ USAF/SEI

1400 Air Force Pentagon

Washington DC 20330-1400

HQ USAF/XON

1480 Air Force Pentagon

Washington DC 20330-1480

Joint Staff/J-4
4000 Joint Staff Pentagon
Washington DC 20318-4000

OATSD (NCB)
3050 Defense Pentagon, 3C125
Washington DC 20301-3050

US Department of Energy, DP-21
PO Box A
Germantown, MD 20874

HQ ACC/SEW
175 Sweeney Blvd
Langley AFB VA 23665-2700

Director of Operations (J-3)
Attn: NOB
3000 Joint Staff Pentagon
Washington DC 20318-3000
HQ AFSPC/SEW
150 Vandenberg St, Ste 1105
Peterson AFB CO 80914-4260

USSTRATCOM/J416
901 SAC Blvd, Ste 1B21/116E
Offutt AFB NE 68113-6300

HQ AFSFC/SFON
1517 Billy Mitchell Blvd
Lackland AFB, TX 78236-0119

DOE/AL/WSD

PO Box 5400

Albuquerque, NM 87185-5400

DTRA-AO/CSNLS

1680 Texas St, SE

Kirtland AFB NM 87117-5669

AAC/NW

1551 Wyoming Blvd, SE

Kirtland AFB NM 87117-5617

HQ AFMC/SE

4375 Chidlaw Rd, Ste 6

Wright-Patterson AFB OH 45433-5006