

**BY ORDER OF THE COMMANDER
341ST MISSILE WING**

341ST MISSILE WING INSTRUCTION 13-501

25 APRIL 2013



Nuclear, Space, Missile, Command and Control

WING INTEGRATION

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 341 MW/CCX

Certified by: 341 MW/SE
(Lt Col Sean P. Boles)

Pages: 8

This instruction complements AFD135, *Air Force Nuclear Enterprise*, 6 Jul 2011. This Missile Wing Instruction (MWI) establishes procedures and terminology to enhance the effectiveness of cross discipline seams. This instruction applies to the 341 MW and all associate units. Air National Guard and Air Force Reserve personnel are exempt from the provisions of this publication. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using AF Form 847, **Recommendation for Change of Publication**; route the AF Form 847 through the wing publishing office. Waivers to this instruction will not be granted. Ensure that all records created as a result of processes prescribed in this publication are maintained IAW Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS). This publication may not be supplemented or further implemented/extended.

1. Overview: This instruction establishes a common baseline of terminology and procedures for critical events that require a high degree of integration. The ability to synchronize the efforts of the numerous moving pieces that support and execute the wing mission requires a significant unity of effort. This instruction will be used as a basis of defining and clarifying commonalities that exist within the missile wing. If the guidance contained within this instruction conflicts with higher-level guidance or technical data, contact the Office of Primary Responsibility (OPR) for resolution.

2. Commander's Intent: This instruction is the byproduct of over a year's worth of Root Cause Analysis (RCA) events at the 341st Missile Wing. A reoccurring theme among these RCA events was inadequate or ineffective communication. As such, the terminology and

guidance contained within this instruction will be incorporated into local training, checklists and guidance.

3. Responsibilities:

3.1. Chief, Wing Weapons and Tactics (341 MW/CCX):

- 3.1.1. Provides a focal point for integration events and opportunities.
- 3.1.2. Oversees the Audit Program as defined in paragraph 5 of this instruction.
 - 3.1.2.1. Provides quarterly schedule for Audit Program.
 - 3.1.2.2. Selects real-world events to review and directs execution.
 - 3.1.2.3. Provides report of discrepancies to 341 MW/CV.
 - 3.1.2.4. Tracks identified fix actions from Audit Program.
- 3.1.3. Serves as a technical advisor/liaison for the 341 MW/CC and the 341 MW/CV.
- 3.1.4. Assists with Missile Wing level hot wash/debrief events (code change, Simulated Electronic Launch-Minuteman (SELM), exercise events, etc).
- 3.1.5. As required, participates in RCA and Air Force Smart Operations for the 21st Century (AFSO21) events that involve more than one group within the wing.
- 3.1.6. Maintains the standardized "LF Debrief Worksheet" used by maintenance teams, the Missile Maintenance Operations Center (MMOC), and the Missile Combat Crew (MCC).

3.2. Chief, Maintenance Group Quality Assurance (341 MXG/QA):

- 3.2.1. Provides evaluator support for the Audit Program.
- 3.2.2. Acts as OPR for Audit Program fix actions associated with the Maintenance Group.

3.3. Chief, ICBM Standardization and Evaluation (341 OG/OGV):

- 3.3.1. Provides evaluator support for the Audit Program.
- 3.3.2. Acts as OPR for Audit Program fix actions associated with the Operations Group.

3.4. Chief, Standardization Evaluation (341 SFG/SFV):

- 3.4.1. Provides evaluator support for the Audit Program.
- 3.4.2. Acts as OPR for Audit Program fix actions associated with the Security Forces Group.

4. Cross Discipline Terminology:

4.1. The following terms are critical to achieve effective communication between the different disciplines related to the Launch Facility (LF) security system. These terms are to be used, as appropriate, whenever an event concerning security is relayed over the telephone or documented in any form of maintenance write-up, log entry or blotter entry.

- 4.1.1. Function Check – A Function Check is initiated by the MCC at a manned LF. A Function Check consists of three critical elements: the triggering and reporting of the

Outer Zone (OZ) alarm, the triggering and reporting of the Inner Zone (IZ) alarm, and the ability to reset both OZ and IZ alarms using Sensitive Command Network Tests (SCNTs) initiated and monitored by the MCC. This definition is derived from the 20AFI31133.

4.1.2. Inoperative (INOP) IZ – An IZ security system is declared inoperative when any of the following conditions exist: incorrectly configured equipment, an incomplete or an unsuccessful Security System Checkout, as defined in TO21MLGM30G24, or when deemed inoperative IAW MMOC or Electromechanical Team (EMT) technical data. An IZ that does not reset following a SCNT may be functional; however it is deemed INOP due to its inability to satisfy nuclear surety requirements per AFI91114. This definition is derived from the TO21MLGM30G24 and TO21M-LGM30G218.

4.1.3. INOP OZ – An OZ security system is declared inoperative when any of the following conditions exist: incorrectly configured equipment, an incomplete or an unsuccessful Security System Checkout, as defined in TO21MLGM30G24, or when deemed inoperative IAW MMOC or EMT technical data. An OZ that does not reset following a SCNT may be functional; however, it is deemed INOP due to its inability to satisfy nuclear surety requirements per AFI91114. This definition is derived from the TO21MLGM30G24 and TO21MLGM30G218.

4.1.4. Operative IZ – The IZ security system can normally be considered operational when the following three conditions are met: (a) the IZ alarm is reset at the Launch Control Center (LCC), (b) the IZ security response to a SCNT is normal at the LCC and (c) the performance and successful completion of all maintenance tasks directed by the TO21MLGM30G24. This definition is derived from the Forward of the TO21MLGM30G24.

4.1.5. Operative OZ – The OZ security system can normally be considered operational when the following four conditions are met: (a) the OZ alarm is reset at the LCC, (b) the OZ security response to a SCNT is normal at the LCC, (c) the performance and successful completion of all maintenance tasks directed by the TO 21MLGM30G24 and (d) the OZ is not considered an Unreliable OZ. This definition is derived from the Forward of the TO21MLGM30G24.

4.1.6. Security System Checkout – A Security System Checkout is performed IAW the TO21MLGM30G24. Anytime a Security System Checkout is required but not successfully completed, the affected security alarms are considered inoperative. The affected security system will remain INOP until the appropriate Security System Checkout is accomplished. An incomplete Security System Checkout can apply to only the IZ or OZ portion of Table 3-1 of TO21M-LGM30G-2-4. A successful IZ Security System Checkout may have an incomplete/unsuccessful OZ Security System Checkout—in this instance the IZ will be operational with an INOP OZ. Anytime there is an incomplete IZ Security System Checkout, the OZ will be considered an Unreliable OZ. Only an EMT or maintenance team authorized by the MXG/CC, with access to the Launcher Equipment Room (LER), can perform the Security System Checkout. This definition is derived from the TO21M-LGM30G-2-4.

4.1.7. Unreliable OZ – An Unreliable OZ is due to an INOP IZ at a site that was penetrated. These conditions cause the radar system portion of the OZ to use an incorrect baseline set of data, thus the OZ is unreliable. An Unreliable OZ is only possible at a site

that has been penetrated and had the security drawer circuit breaker cycled. This definition is derived from the TO21M-LGM30G-2-4.

4.1.8. True Status – Status reported by the security system that accurately represents the security condition of the site. True status is verified by the appropriate security system functional checks, proper LF back out procedures and proper system response to SCNTs sent by the MCC (TO21M-LGM30G-1-24 allows up to three SCNTs to get a good reset). This definition was provided by the Air Force Safety Center.

4.2. The following terms are used to define alert status of a LCC or an LF:

4.2.1. Fully Mission Capable (FMC) – The system or equipment is functioning as required in TO specifications and is capable of performing all of its assigned missions. This definition is derived from AFI21-103.

4.2.2. Not Mission Capable (NMC) – The system or equipment does not meet the TO specifications; therefore, cannot accomplish any of its assigned missions or functions. This definition is derived from AFI21-103.

4.2.3. Partially Mission Capable (PMC) – System or equipment functioning in such a way that it can perform at least one, but not all of its assigned missions; functions impaired but usable. Systems with redundant capabilities will be coded PMC when redundancy is lost, even though the system is fully capable of supporting all of its assigned missions. This definition is derived from AFI21-103.

4.2.4. Off-Alert – Sortie is non-launch capable, directed to be off alert IAW Crew Document Annotation Procedure (CDAP) or is in a condition requiring off alert status as determined by MMOC. An Off-Alert sortie is considered NMC. This definition is derived from the glossary of AFGSCI135304.

4.2.5. Crew Document Annotation Procedure (CDAP) – Procedure that prevents an Intercontinental Ballistic Missile (ICBM) from launching with an incorrect delay time, on an incorrect target or with a hardware condition that could prevent it from reaching its OPLAN target. This definition is derived from the glossary of AFGSCI135304.

4.2.5.1. Hardware Off-Alert – A launch capable sortie off alert due to a hardware problem that prevents launch against a strategic target until the condition is corrected. For example, a launch capable sortie with a stuck Safety Control Switch (SCS) key would be called Hardware Off-Alert. This is because the missile would be able to process critical launch commands. By processing these commands, the Missile Guidance Set (MGS) will abort terminal countdown and shutdown due to the SCS key. This will further delay the ability of returning the sortie to a FMC state. Another variant of Hardware Off-Alert would be if incorrect software, programs or tapes were loaded into an operational LF. This definition is derived from the glossary of AFGSCI135304.

4.2.5.2. Targeting Off-Alert – A sortie that has incorrect targeting, that cannot be resolved, will be considered Targeting Off-Alert. Situations would include: (a) the inability to Remote Data Change (RDC) targeting case data or Execution Plan (EP) case data to a sortie at case effective time due to a condition at the LF, (b) an input abort of target case or EP case data, (c) a generation abort of target case or EP case

data and (d) when a planned Re-entry System (RS) configuration change does not occur by targeting case effective time. This definition is derived from the HITTF 214.

5. Audit Program:

5.1. The Audit Program is used to ensure that an accurate site picture is maintained between the Maintenance Group (MXG), the Operations Group (OG), and the Security Forces Group (SFG) regarding the security systems used at LF. A goal of the Audit Program will be to identify processes or policies that can be refined to improve the effectiveness of cross organization communication and interaction.

5.2. Program Requirements:

5.2.1. At least three audits will be performed per quarter with support from 341 MXG/QA, 341 OG/OGV and 341 SFG/SFV.

5.2.2. Results of the Audit Program will be briefed by the Chief, Wing Weapons and Tactics to the 341 MW/CV upon completion of the audit.

5.2.3. The Audit Program will review the following events, as applicable, for compliance, accuracy, completeness and timeliness:

5.2.3.1. Security Situation Declaration.

5.2.3.2. Request for a Camper Alert Team (CAT).

5.2.3.3. LF Site Debrief Worksheet.

5.2.3.4. Release for a CAT.

5.3. Upon selection of a real-world event, all materials related to that LF will be reviewed from the initial event to the time of site selection. All available means to verify compliance, accuracy, completeness and timeliness must be exhausted during the audit to include, at a minimum, the following items:

5.3.1. MCC Crew Log and Operator Entered Status (OES) entries.

5.3.2. Integrated Maintenance Data System (IMDS) work orders.

5.3.3. Missile Maintenance Operations Center (MMOC) Senior Controller log.

5.3.4. Security System Air Force Technical Order (AFTO) Forms 42, as appropriate.

5.3.5. Missile Security Control (MSC) blotter entries.

5.3.6. Flight Security Controller (FSC) blotter entries.

5.3.7. Recorded phone calls.

5.4. All materials generated by the Audit Program will be maintained IAW AFI10701, *Operational Security (OPSEC)* and DoDM 5200.01 Vol 4, *DoD Information Security Program: Controlled Unclassified Information*.

6. Missile Field Communications

6.1. All communications regarding maintenance actions or a potential contingency event at a LF between a maintenance team chief and the MMOC will have the appropriate primary MCC patched in. This includes when MMOC is calling the team chief.

ROBERT W. STANLEY II, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

20AFI 31133, *Intercontinental Ballistic Missile (ICBM) Systems Security*
 AFGSCI135304, *EWO Generation and Targeting – ICBM (GATI)*
 AFI10701, *Operational Security (OPSEC)*
 AFI21103, *Equipment Inventory, Status and Utilization Reporting*
 AFI21202v1_AFGSCSUP, *Missile Maintenance Management*
 AFI91114, *Safety Rules for the Intercontinental Ballistic Missile System*
 DoDM 5200.01 Vol 4, *DoD Information Security Program: Controlled Unclassified Information*
 HITTF 214, *OPLAN 8010 Handbook for ICBM Targeting-Task Force 214*
 TO21MLGM30F121, *Minuteman Nuclear Surety Procedures for the WS-133A-M/B Weapon Systems*
 TO21MLGM30G124, *Minuteman Weapon System – Wings I, III, and V (Rapid Execution and Combat Targeting) USAF Series LGM30G Missile*
 TO21MLGM30G218, *Organizational Maintenance Control, Minuteman Weapon*
 TO21MLGM30G24, *Organizational Maintenance Instructions Launch Facility Security System Wing I, III, V, and Peacekeeper*

Prescribed Forms

None

Adopted Forms

AF Form 847, **Recommendation for Change of Publication**

Abbreviations and Acronyms

AFSO21—Air Force Smart Operations for the 21st Century
AFTO—Air Force Technical Order
CAT—Camper Alert Team
CDAP—Crew Document Annotation Procedure
EMT—Electromechanical Team
FMC—Fully Mission Capable
FSC—Flight Security Controller
ICBM—Intercontinental Ballistic Missile
IMDS—Integrated Maintenance Data System
INOP—Inoperative

IZ—Inner Zone
LCC—Launch Control Facility
LER—Launcher Equipment Room
LF—Launch Facility
MCC—Missile Combat Crew
MGS—Missile Guidance Set
MMOC—Missile Maintenance Operation Center
MSC—Missile Security Control
MXG—Maintenance Group
NMC—Not Mission Capable
OES—Operator Entered Status
OG—Operations Group
OPLAN—Operational Plan
OPR—Office of Primary Responsibility
OPSEC—Operational Security
OZ—Outer Zone
PMC—Partially Mission Capable
RCA—Root Cause Analysis
SCNT—Sensitive Command Network Test
SCS—Safety Control Switch
SELM—Simulated Electronic Launch-Minuteman
SFG—Security Forces Group