

31 OCTOBER 2001

Operations



**ELECTRONIC WARFARE INTEGRATED
REPROGRAMMING**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: HQ USAF/XOIE (Maj Peter Bloom)

Certified by: HQ USAF/XOI
(Maj Gen Glen D. Shaffer)

Supersedes AFI 10-703, 1 July 1996.

Pages: 68
Distribution: F

This instruction implements Air Force Policy Directive (AFPD) 10-7, *Command and Control Warfare*, by providing the requirements to reprogram electronic warfare/informational warfare (EW) systems in response to changing threats. Because electronic warfare integrated reprogramming (EWIR) requires multiple agencies to work together, each agency must ensure its reprogramming is timely, accurate, and effective. These instructions implement portions of the Chairman of the Joint Chiefs of Staff (CJCS) Instruction CJCSI 3210.03 *Joint Electronic Warfare Policy*, 10 January 2000; MJCS; CJCSI 3212.04 *Joint Coordination of Electronic Warfare (EW) Reprogramming Policy and Procedures*, 14 December 2000 (Draft); and Joint Pub 3-51, *Joint Doctrine for Electronic Warfare*, April 7, 2000. **Records Disposition.** Ensure that all records created by this AFI are maintained and disposed of IAW AFMAN 37-139, *Records Disposition Schedule*. See **Attachment 1** for a glossary of abbreviations, acronyms, and terms used in this instruction.

SUMMARY OF REVISIONS

This document is substantially revised and must be completely reviewed.

Tasked assigned to MAJCOM, DRU, FOA, and individual units have been changed to reflect current operating procedures. Additional units that have been formed since last revision have been included. New message formats have been developed and included.

Chapter 1—EWIR PURPOSE, OBJECTIVES, PROCESS AND SECURITY	4
1.1. Purpose.	4
1.2. Objectives.	4
1.3. EWIR Process.	4
Figure 1.1. EWIR Process.	5

1.4. Security Precautions.	6
Chapter 2—FUNCTIONAL RESPONSIBILITIES	8
2.1. Air Staff:	8
2.2. MAJCOMs and Agencies.	10
2.3. 53d Wing (53d Electronic Warfare Group) and Air Force Special Operations Command Electronic Combat Support Flight (AFSOC/ECSF) Operational Reprogramming Centers:.....	16
2.4. Air Force Materiel Command (AFMC) (Reprogramming Center [RC]).	17
2.5. Air Force Operational Test and Evaluation Center (AFOTEC).	18
2.6. Air Intelligence Agency (AIA):	18
2.7. Air Force Air Operations Center (AOC).	20
2.8. EWIR Committee and Subcommittee Interoperability:	21
Chapter 3—OPERATIONAL PROCEDURES	23
3.1. EWIR Deficiency Reporting.	23
3.2. Implementing Changes.	24
3.3. Timeliness of Reprogramming Actions.	26
Chapter 4—EXERCISES AND EVALUATION PROGRAMS	28
4.1. General.	28
4.2. Air Force Directed Exercises.	28
4.3. MAJCOM Directed Exercises.	29
4.4. Local Exercises.	29
Chapter 5—INTERNATIONAL AGREEMENTS AND SECURITY ASSISTANCE	30
5.1. Purpose.	30
5.2. Scope.	30
5.3. Objectives.	30
5.4. Special Factors.	30
5.5. EW Systems Support	31
5.6. Programs.	31
5.7. Functional Responsibilities.	31
5.8. US Air Force Management:	35
5.9. Operational Procedures.	37

AFI10-703 31 OCTOBER 2001	3
5.10. Intelligence.	37
5.11. Communications.	37
5.12. Support.	37
Attachment 1—GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION	39
Attachment 2—EWIR SUBCOMMITTEE MEMBERSHIP MATRIX	46
Attachment 3—SAMPLE FLAGGING REPORT (FLR) FORMAT	47
Attachment 4—SAMPLE OPERATIONAL CHANGE REQUEST (OCR) FORMAT	49
Attachment 5—SAMPLE SOFTWARE CANGE MESSAGE (SCM) FORMAT	51
Attachment 6—SAMPLE SYSTEM IMPACT MESSAGE (SIM) FORMAT	53
Attachment 7—SAMPLE REPROGRAMMING IMPACT MESSAGE (RIM) FORMAT	55
Attachment 8—SAMPLE MAINTENANCE INSTRUCTION MESSAGE (MIM) FORMAT	57
Attachment 9—SAMPLE TIME COMPLIANCE TECHNICAL ORDER MESSAGE (TCTO) FORMAT	59
Attachment 10— SAMPLE IMPLEMENTATION MESSAGE (IMP) FORMAT	61
Attachment 11—SAMPLE UNIT LOADING MESSAGE (ULM) FORMAT	63
Attachment 12—SAMPLE STATUS MESSAGE (STM) FORMAT	65
Attachment 13—EWIR MESSAGE DESIGNATION STANDARDS FOR THE SUBJECT LINE	67

Chapter 1

EWIR PURPOSE, OBJECTIVES, PROCESS AND SECURITY

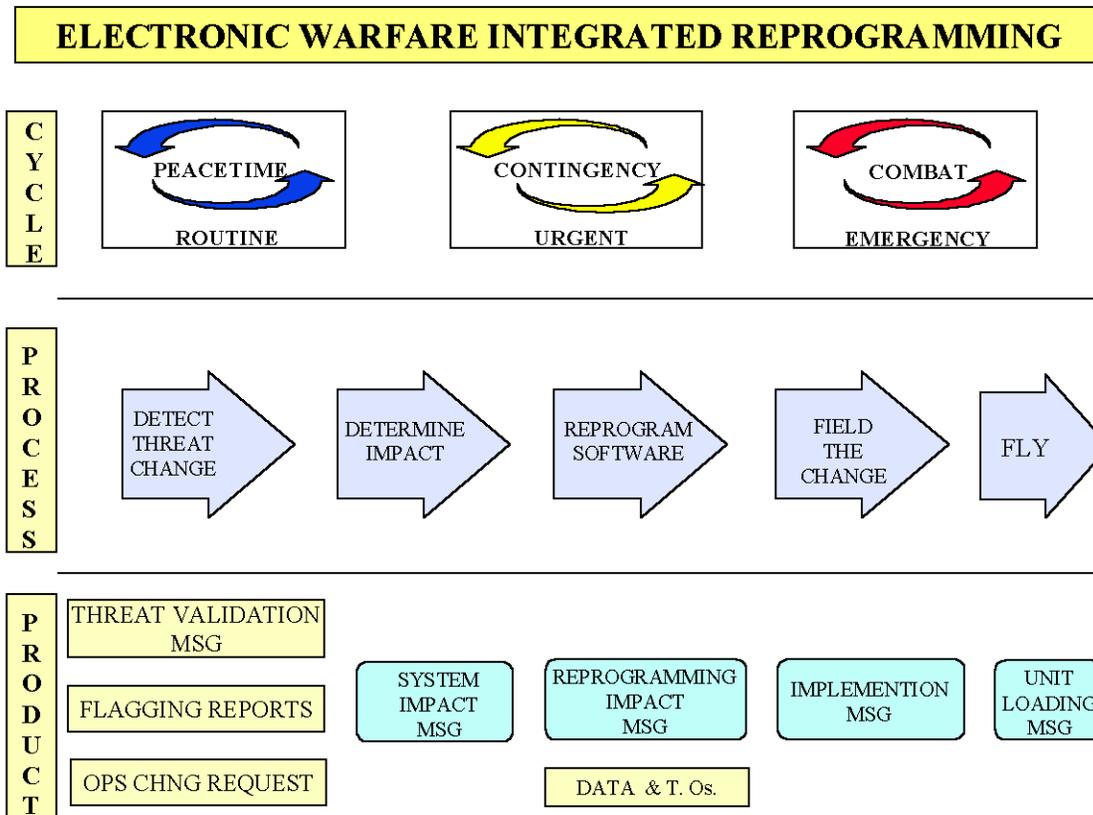
1.1. Purpose. Electronic Warfare Integrated Reprogramming (EWIR) is a systematic decision-making tool for operational commanders. It gives all Air Force units a timely and accurate means to respond to expected and unexpected electronic emissions, changes in air defense tactics, and unique mission requirements. These EWIR responsibilities include procedures for changes in tactics, employment guidance, electronic warfare (EW) equipment (software/hardware), aircrew training and training devices (i.e. threat simulators, threat emitters) and other support systems.

1.2. Objectives. The Air Force's EWIR objective is to increase combat/mission survivability (C/M S). In order to meet this, the Air Force must maintain the ability to detect, classify, and effectively counter adversaries' air defenses in support of Combat Air Force (CAF), Special Operations Forces (SOF), Mobility Air Forces (MAF), and Foreign Military Sales (FMS) assets. To support this objective, the Air Force must:

- 1.2.1. Maintain an effective intelligence capability to rapidly collect, identify, compare, analyze, and distribute all-source intelligence information during peacetime, contingency, and wartime operations.
- 1.2.2. Support an accurate, timely, and worldwide EWIR database (EWIRDB) providing intelligence, operations and acquisition personnel with parametric data for EW systems reprogramming.
- 1.2.3. Support order of battle (OB) databases for regions by providing an "electronic fit" (EW-system-to-weapon-system-platform correlation) of threats to generate regional mission data (MD).
- 1.2.4. Maintain an effective and responsive wartime reserve and threat analysis capability.
- 1.2.5. Develop and implement EWIR support structures and processes that includes tactics, employment guidance, doctrine, training, effective operational responses to enemy actions and operate an effective EWIR training program at all command levels.
- 1.2.6. Establish and implement a timely, secure, and survivable means to push and/or pull reprogramming change information worldwide. This means must support the warfighter's sortie generation rate.
- 1.2.7. Maintain facilities and equipment to create, test, and distribute EW software changes for operational commanders.
- 1.2.8. Develop research, development, test, and evaluation (RDT&E) resources to obtain rapidly reprogrammable EW systems, improve existing EW systems, and related support equipment that remains effective in a changing electromagnetic environment.
- 1.2.9. Promote joint applications and interoperability.
- 1.2.10. Establish reach back procedures and mechanisms that allow commanders to get support for EWIR related issues.

1.3. EWIR Process. The EWIR process is, in simplistic terms, made up of four different steps. These steps are: 1) determine the threat; 2) determine the impact on EW systems; 3) reprogram the EW system's software; and 4) field the software change.

Figure 1.1. EWIR Process.



1.3.1. Determine the threat:

1.3.1.1. The intelligence community collects and evaluates a wide variety of data on threat systems through all source intelligence, and reports this to the reprogramming centers (RCs) as well as other agencies. They also allow RCs to determine a threat’s impact on EW systems during a Foreign Materiel Exploitation (FME) (ref. AFI 99-114). Intelligence (Red, Gray) and Blue parametric data are consolidated and provided to RCs in the EWIR Data Base (EWIRDB) and other analytical reports, which is used to program EW systems. The EWIRDB or its replacement shall include data on red, blue, and gray systems.

1.3.1.2. Intelligence is filtered manually or through EW systems computer flagging models to determine what threats have changed. This begins the process to determine how the change impacts on the EW systems. Service Production Centers (SPCs) then validate the change as an actual operational mode of the threat system.

1.3.2. Determine the impact on EW systems:

1.3.2.1. RCs continue the process of assessing the threat change impact on an EW system by performing engineering analysis, as well as laboratory and flight testing.

1.3.2.2. The RC, in coordination with the affected major commands (MAJCOMs) and/or the Joint Forces Air Component Commander (JFACC)/Combined Forces Air Component Commander (CFACC)/Air Force Air Operations Center (AOC), determines how to respond to the threat change. The response may be:

- no action
- a change to existing tactics
- reprogramming the MD or system software
- change existing hardware
- or acquire new hardware

The RC reports the impact of the threat change, the effect on the EW system, an interim course of action, and recommended course of action to the units, the MAJCOM and JFACC/CFACC/AOC in a System Impact Message (SIM). Critical messages may warrant verbal contact with the units, MAJCOM and/or JFACC/CFACC/AOC to facilitate “pulling” information from the Data Distribution System (DDS).

1.3.3. Reprogram the EW system’s software:

1.3.3.1. If changing the EW systems MD and/or system software is the determined course of action, the RCs:

1.3.3.1.1. Develop the software change.

1.3.3.1.2. Test the change in the laboratory (hardware-in-the-loop, computer simulation, or critical analysis).

1.3.3.1.3. Flight test the change, if required.

1.3.3.1.4. Recommend fielding the software change to the MAJCOM and/or JFACC/CFACC/AOC.

1.3.3.1.5. Provide changes to AFIWC (453 EWS) so flagging models can be updated.

1.3.4. Field the MD and/or system software change:

1.3.4.1. After coordinating with the MAJCOM and/or JFACC/CFACC/AOC, the RCs distribute the software change to the field electronically and post it on the appropriate BBS. Additionally, maintenance installation instructions are sent in a Maintenance Instruction Message (MIM) or Time Compliance Technical Order (TCTO). A description of the operational impact of the software change on the EW system is sent to the MAJCOM and/or JFACC/CFACC/AOC and field units in a Reprogramming Impact Message (RIM).

1.3.4.2. The MAJCOM and/or JFACC/CFACC/AOC use the RIM, along with previous coordination with RCs, to determine whether to install the new software in their units' EW equipment and the priority used to implement the change. If the MAJCOM and/or JFACC/CFACC/AOC decide to install the software, they direct the installation using an Implementation Message (IMP).

1.3.4.3. Once units have installed the software in their EW systems, they report this to their MAJCOM and/or JFACC/CFACC/AOC and the RCs using the Unit Loading Message (ULM) within 72 hours of completion, indicating implementation status and issues affecting 100% aircraft upload.

1.4. Security Precautions. At all levels of the EWIR process:

1.4.1. Follow all applicable security classification guides for EWIR database with each EW system and its host platform. The guides should include, but not limited to, *DOD Threat Simulator Program*

Security Classification Guide, March 1998, Defense Intelligence Agency, Missile and Space Intelligence Center, Redstone Arsenal, AL and the Electronic Warfare (EW) Threat Emitter Security Classification Guide Range Threat Systems, Ogden Air Logistics Center (OO-ALC) Hill AFB UT 84056-5838).

1.4.2. Follow operations security (OPSEC) and communications security (COMSEC) at all times.

Chapter 2

FUNCTIONAL RESPONSIBILITIES

2.1. Air Staff:

2.1.1. HQ USAF/XO. The Deputy Chief of Staff for Air and Space Operations:

2.1.1.1. Manages EWIR activity.

2.1.1.2. Prepares and implements EWIR-related program management directives (PMD).

2.1.1.2.1. Groups all EWIR acquisition programs and funding under a single Electronic Warfare Avionics Integration Support Facility (EWAISF) PMD.

2.1.1.2.2. Acts as the EWAISF PMD program officer by writing and updating PMD 5092 in accordance with (IAW) applicable directives.

2.1.1.2.3. Approves and manages EWAISF funding.

2.1.1.3. Resolves EWIR conflicts at the MAJCOM level via the EWIR Oversight Committee.

2.1.1.4. Chairs the EWIR Oversight Committee.

2.1.1.5. Ensures MAJCOMs, JFACC/CFACC/AOCs, and RCs effectively communicate their EWIR intelligence production requirements to the intelligence community and HQ USAF/XOI.

2.1.1.6. Ensures the Air Force trains, practices, and evaluates all phases of the EWIR process annually by conducting a worldwide exercise. To the maximum extent possible, reprogramming exercises should be conducted as part of a major joint exercise, allowing joint and service components the opportunity to exercise the reprogramming process together.

2.1.1.6.1. Coordinates with the joint staff the inclusion of emergency reprogramming objectives in future joint task force (JTF) level exercises.

2.1.1.6.2. Selects and tasks the participating MAJCOM to function as the Air Force lead to plan, implement, and manage the reprogramming process.

NOTE: This requirement may be satisfied by a major PACER WARE action involving most US Air Force EW systems.

2.1.1.7. Oversees the analysis of EW equipment based on potential threats or enemy threat change validations.

2.1.1.8. Develops AF procedures and coordinates with other services for jointly developing and using EWIR resources.

2.1.1.9. Co-chairs the Foreign Military Sales (FMS) Electronic Combat Working Group (ECWG) or Information Operations Working Group (IOWG), which manages policies and procedures for transferring US Air Force EW capabilities to allied and friendly nations.

2.1.1.10. Ensures that the capabilities of all FMS systems/programs are captured for inclusion in the EWIR database, so that US forces engaged with these allies will be able to prevent fratricide incidents.

2.1.1.11. Oversees the FMS Electronic Combat International Security Assistance Program (ECISAP) as described in [Chapter 5](#).

2.1.1.12. Ensure that AF components participates in all appropriate FME testing and analysis.

2.1.2. HQ USAF/XOI. The Director of Intelligence, Surveillance and Reconnaissance:

2.1.2.1. Ensures AFIWC (453 EWS), in conjunction with the other services, provides data on blue systems to the National Air Intelligence Center (NAIC) for inclusion in EWIRDB.

2.1.2.2. Works with the DIA, SAF/IAW, and the Joint Staff to set up procedures for rapidly validating and reporting threat changes.

2.1.2.3. Ensures the MAJCOMs, JFACC/CFACC/AOCs, and RCs document their operational EWIR intelligence requirements and sends them to the Defense Intelligence Agency (DIA) for action. Also acts as an advocate for their completion.

2.1.2.4. Works with the DIA to ensure other services and intelligence agencies receive EWIR intelligence support.

2.1.2.5. Supports intelligence production requirements unique to the EWIR process.

2.1.2.6. Works within the intelligence community and AFIWC (453 EWS) to provide EWIR products for the RCs to support allied and friendly nations.

2.1.2.7. Coordinates the EWIR efforts of the DIA, JICs, JAC, and EWIRDB production centers in IAW CJCSI 3212.04.

2.1.2.8. Ensure that results from FME testing and analysis are provided to RCs and SPCs in a timely manner.

2.1.2.9. Ensures SPCs communicate information with the RCs.

2.1.2.10. Serves as OPR for staffing emergency reprogramming change release to FMS customers for which disclosure guidance has not been delegated.

2.1.3. HQ USAF/IL. The Deputy Chief of Staff for Logistics:

2.1.3.1. Establishes logistical policy to support and sustain Air Force EWIR equipment.

2.1.3.2. Assists in the identification, definition, and integration of the user's operational and technical requirements of EWIR Automatic Test Systems (ATS) support tools for system software and MD.

2.1.3.3. Ensures user needs (reliability, maintainability, reprogrammability, and deployability) are addressed in the acquisition and development of EWIR-related ATSS.

2.1.3.4. Advocates and ensures users' EWIR supportability and sustainment needs are addressed in the action and processes of the Central ATS Product Group Management Office (WR-ALC/LEA).

2.1.3.5. Assists in the identification and resolution of EWIR-related ATS logistics and sustainability issues.

2.1.3.6. Serves as an advisor to the EWIR Communication Subcommittee and advocates the committee's recommendations.

2.1.3.7. Assists the RCs' participation in Foreign Materiel Exploitation (FME).

2.1.4. HQ USAF/SC. Deputy Chief of Staff, Communications and Information:

2.1.4.1. Provides technical assistance on all EWIR communications-computer requirements.

2.1.4.2. Assist WR-ALC/LN, MAJCOMs, and RCs in developing and maintaining a comprehensive EWIR communications plan outlining current and future connectivity to common-user, base-level, and long-haul communications systems.

2.1.4.3. Coordinates with HQ USAF/XOIE on communications issues unique to EWIR data.

2.1.4.4. Serves as an advisor to the EWIR Communications Subcommittee and advocates the committee's recommendations.

2.1.5. SAF/IA. The Deputy Under Secretary for International Affairs:

2.1.5.1. Acts as the focal point for the sale of US Air Force EW and EWIR systems to allied and friendly nations.

2.1.5.2. Informs the JCS and unified commanders of proposed and actual sales of EW systems (to include hardware and software configurations) to allied and friendly nations.

2.1.5.3. Acts as the OPR for transferring military information to allied and friendly nations.

2.1.5.4. Co-chairs the FMS ECWG to manage policies and procedures for transfer of US Air Force EW capabilities to allied and friendly nations.

2.1.5.5. Provides oversight to the FMS ECISAP as described in [Chapter 5](#).

2.1.5.6. Acts as focal point for releasing USAF technology to allied forces.

2.1.5.7. Formulates and staffs coordinated and cohesive FMS National policy in coordination with the other services.

2.1.6. SAF/AQ. The Deputy Under Secretary for Acquisition:

2.1.6.1. Ensures all new acquisitions are compatible with the EWIR process.

2.1.6.2. Ensures all PMDs direct the implementation of appropriate system hardware and software designs that facilitate EWIR and the concurrent delivery of reprogramming support tools which are compatible with EWIR.

2.1.6.3. Represents EWIR acquisition policy in joint service initiatives.

2.1.6.4. Disseminates EWIR acquisition strategy and policy to all Air Force acquisition offices.

2.1.6.5. Assists the RCs' participation in FME.

2.2. MAJCOMs and Agencies. Air Combat Command (ACC), Air Education and Training Command (AETC), Air Force Special Operations Command (AFSOC), Air Mobility Command (AMC), Air Force Materiel Command (AFMC), Air Force Space Command (AFSPC), Air Intelligence Agency (AIA), US Air Forces Europe (USAFE), Pacific Air Forces (PACAF), Air Force Operational Test and Evaluation Center (AFOTEC), Air Force Reserve Command (AFRC) and the National Guard Bureau (NGB)

2.2.1. Common MAJCOM and Agencies tasks:

- 2.2.1.1. Provide staffing, resources, and funding to fulfill peacetime, wartime, contingency, and exercise EWIR requirements.
- 2.2.1.2. Advise the Chief of Staff, Headquarters US Air Force (HQ USAF), when EWIR capabilities do not meet Air Force objectives.
- 2.2.1.3. Ensure comprehensive EWIR training programs, which include EWIR decision-making and intelligence support, are developed.
- 2.2.1.4. Ensure Operational Plans (OPLANs), Contingency Plans (CONPLANs), and strategic war plans discuss EWIR in order to:
 - 2.2.1.4.1. Encourage effective exchange of information.
 - 2.2.1.4.2. Eliminate duplication of effort.
 - 2.2.1.4.3. Achieve mutual joint service support in accordance with Joint Pub 3-51.
 - 2.2.1.4.4. Incorporate lessons learned from past reprogramming actions.
- 2.2.1.5. As directed by USAF/XO, assume the lead for planning, implementing, and managing the Air Force reprogramming efforts during the selected joint level exercise chosen to evaluate the EWIR process. This responsibility may be delegated to the combatant Numbered Air Force (NAF) participating as the Air Force component to the joint exercise.
 - 2.2.1.5.1. Conduct exercise planning conferences and EWIR conferences, as required.
 - 2.2.1.5.2. Develop the reprogramming goals and objectives for the Air Force components.
 - 2.2.1.5.3. Coordinate with the AFIWC (453 EWS), who coordinates exercise planning and logistical support.
 - 2.2.1.5.4. Ensure exercise participants identify, collect, and report critical EWIR elements.
 - 2.2.1.5.5. Consolidates major findings and lessons learned. Using the Joint Universal Lesson Learned System (JULLS) format, report findings and lessons learned as part of the overall Air Force/Joint exercise report.
 - 2.2.1.5.6. Suggest improvements with memo to the EWIR Oversight Committee.
 - 2.2.1.5.7. Identify the EW systems and units requiring reprogramming exercises and coordinates this information with the AFIWC (453 EWS) and the RC's.
- 2.2.1.6. Conduct MAJCOM directed reprogramming exercises to train and evaluate operational, maintenance, and communications personnel, and their procedures.
 - 2.2.1.6.1. Include the appropriate gained units in reprogramming exercises.
 - 2.2.1.6.2. Compile exercise results and recommendations and send them to the appropriate agencies.
- 2.2.1.7. Develop EWIR hardware and software requirements and coordinate them with other MAJCOMs and HQ USAF/XO. These requirements include:
 - 2.2.1.7.1. Data automation
 - 2.2.1.7.2. Test capabilities
 - 2.2.1.7.3. Communication connectivity

2.2.1.7.4. Support equipment

2.2.1.7.5. Bulletin Board Systems

2.2.1.8. Provide applicable RCs with annual updates of the EW assets and locations.

2.2.1.9. Ensure RC's EWIR information requirements on threat systems, including Wartime Reserve Mode (WRM), are current, complete, and properly documented.

2.2.1.10. Ensure Urgent or Emergency PACER WARE changes are given the highest range scheduling priority possible.

2.2.1.11. Provide operational requirements/oversight to the development, test, distribution, and loading of MD and system software changes.

2.2.1.12. Ensure that operational units are aware of and follow the proper content, format, and routing of OCR's (Operational Change Requests) to effect changes in EW equipment.

2.2.1.13. Provide oversight of the fielded EW systems to ensure that they meet the hardware, software, and MD configuration standards set by the RCs and endorsed by the Headquarters.

2.2.1.14. Support all appropriate FME by ensuring requirements are provided to appropriate organizations and RC participation in planning and execution of testing and analysis.

2.2.2. Operations Directorate (DO) or Equivalent:

2.2.2.1. Oversees EW reprogramming.

2.2.2.2. Approves software changes for all EW systems fielded in their area of responsibility (AOR).

2.2.2.3. Considers recommendations from the RCs.

2.2.2.4. Sends Implementation Messages (IMP) to applicable units, with informational copies to other MAJCOM and CFACC/JFACC/AOC staffs, and the RCs (not applicable to NGB and AFRC).

2.2.2.4.1. Coordinate within the MAJCOM directorates prior to sending IMPs to insure that maintenance tech data changes are available, if applicable.

2.2.2.5. Upgrades EW software flight-testing priorities during wartime and contingency operations.

2.2.2.6. Discusses employment and operational concepts for the assets in their AOR with the RCs.

2.2.2.7. Supports the ECISAP, as requested.

2.2.2.8. Conducts, manages, and supports all force development evaluation required to fully evaluate all EW software or MD changes.

2.2.2.9. Works with AFIWC (453 EWS) to identify flagging model requirements.

2.2.2.10. Works with the RCs to identify initial and upgrade requirements and funding for reprogramming facilities, equipment, and manpower support, for EW systems currently fielded or under development.

2.2.2.10.1. Works with the RCs to ensure changes to fielded EW systems, support equipment, and new systems are compatible with EWIR requirements and associated communications support systems.

2.2.2.10.2. Ensures reprogramming facilities, equipment, and staffing for these changes are current, adequate, and funded.

2.2.2.10.3. Supports force development evaluation required to fully evaluate all EW software or MD changes.

2.2.2.11. Ensures field units receive adequate EW support equipment.

2.2.3. Requirements and Acquisition Directorate (DR) or Equivalent:

2.2.3.1. Coordinates EW system requirements.

2.2.3.2. Ensures all applicable program specifications include validated operational requirements.

2.2.3.3. Represents program management concerns during the demonstration and validation, engineering and manufacturing development, and production and deployment phases of acquisition.

2.2.3.4. Monitors EW equipment and support equipment to ensure units are have adequate EWIR logistics support.

2.2.3.5. Coordinates with platform System Program Office to insure that technical order changes caused by PACER WARE updates are being accomplished.

2.2.3.6. Ensures maintenance personnel receive training in reprogramming EW systems.

2.2.3.7. Identifies and coordinates Operational Test and Evaluation (OT&E) requirements with AFOTEC for all EW systems.

2.2.4. Communications and Information Directorate (SC) or Equivalent:

2.2.4.1. Provide guidance to communications squadrons on means to push or pull PACER WARE and SERENE BYTE messages.

2.2.4.2. Serves as an advisor to the EWIR Communications Subcommittee and advocates the committee's recommendations.

2.2.5. Intelligence Directorate (IN) or Equivalent:

2.2.5.1. Ensure resources and personnel are programmed to support the MAJCOM EWIR intelligence (i.e. collection, threat assessment, etc.) requirements.

2.2.5.2. Ensure the RCs document their operational EWIR intelligence requirements and send them to the DIA for action. Also acts as an advocate for their completion. (As required).

2.2.6. Numbered Air Forces (NAF):

2.2.6.1. Monitor theater operations and intelligence data to identify and assess changes in the EW environment.

2.2.6.1.1. Review and forward aircrew and electronic support inputs on threat parameter changes and new threats in their AOR to appropriate MAJCOM, RCs, and AFIWC for further review and analysis.

2.2.6.2. Support implementation of:

2.2.6.2.1. Software changes

2.2.6.2.2. Equipment settings

2.2.6.2.3. Aircrew tactics changes

2.2.6.3. Verify aircrews receive the appropriate SIMs and RIMs.

2.2.6.4. Ensure appropriate plans; instructions, and responsibilities for EW reprogramming are disseminated at the appropriate levels.

2.2.6.5. Participate in and support reprogramming exercises as directed by the MAJCOM.

2.2.7. Wing/Group:

2.2.7.1. Assign a primary and alternate EW point of contact (POC). EW POC must be the Wing/Group Electronic Combat Officer (ECO), Wing/Group EW Officer (EWO), or Wing/Group Electronic Combat Pilot (ECP) to coordinate EWIR activities.

2.2.7.2. Set up an EWIR action team consisting of operations, maintenance, intelligence, and communications personnel to:

2.2.7.2.1. Develop plans and instructions to implement reprogramming tasks.

2.2.7.2.2. Develop procedures for receiving, sending and distributing reprogramming messages both at home station and deployed locations.

2.2.7.2.2.1. Ensure access to applicable RCs BBS.

2.2.7.2.2.2. Establish a Defense Message System (DMS) functional account (classified and unclassified, as required) for the Wing/Group. Ensure required actions are completed on a routine basis to ensure messages can be delivered at anytime.

2.2.7.2.3. Immediately report any errors in reprogramming procedures to the MAJCOM and RC representatives.

2.2.7.3. Produce and staff OCRs IAW paragraph 3.1. to enhance or correct system operations.

2.2.7.4. Participate in reprogramming exercises as directed.

2.2.7.4.1. Report reprogramming exercise results in accordance with paragraph 3.2.

2.2.7.5. The EW POC (Wing/Group WSO/EWO/ECP):

2.2.7.5.1. Directs the Wing/Group EWIR action team.

2.2.7.5.2. Review findings of anomalies from Wing/Group IN (see section 2.2.11.10.2) and prepares an OCR when discrepancies are found.

2.2.7.5.3. Ensures aircrews are informed of current EW equipment capabilities by using all available sources, including:

2.2.7.5.3.1. Test plans

2.2.7.5.3.2. Test results

2.2.7.5.3.3. PW Messages

2.2.7.5.3.4. System handbooks or EC mission guides

2.2.7.5.3.5. Air Force Tactics Techniques and Procedures (AFTTP) 3-1

2.2.7.5.4. Is responsible for a process that will notify the Wing/Group EWIR action team when EWIR messages have been received.

2.2.7.5.4.1. Is the owner of the Wing/Group PW DMS account.

2.2.7.5.5. Works with the operations group (OG) (or equivalent) to prioritize EW equipment software or hardware changes.

2.2.7.5.6. Sends all required EWIR reports and messages to higher headquarters and subordinate organizations, as appropriate.

2.2.7.5.7. Maintains a current listing of operational and training software for each of the Wing/Group's EW systems.

2.2.7.5.8. Notifies MAJCOM and RCs of connectivity status for EWIR activity.

2.2.7.6. Aircraft and Maintenance Squadrons:

2.2.7.6.1. Ensure required EW reprogramming equipment is available and operational (such as STU-III/STE, DCS, PLV, MLV, CAPRE) to support reprogramming at home and deployed locations. If not, notify the Wing/Group WSO/EWO/ECP.

2.2.7.6.2. Ensure adequate personnel have access to the appropriate RC's BBS to conduct actual and exercise reprogramming actions both at home station and deployed locations.

2.2.7.6.3. Implement changes only after Wing/Group WSO/EWO/ECP's approval.

2.2.7.6.3.1. Keep the Wing/Group WSO/EWO/ECP informed of changes and provide timing data, as required.

2.2.7.6.4. Participate in the EWIR action team.

2.2.7.7. The Wing/Group IN:

2.2.7.7.1. Provides the Wing/Group WSO/EWO/ECP with threat changes that may impact EW systems and includes this information, along with PW messages, in aircrew mission briefings.

2.2.7.7.2. Reviews aircrew debriefings and mission reports for EW equipment anomalies, which may indicate threat parameter changes and reports these findings to the Wing/Group WSO/EWO/ECP for action.

2.2.7.7.2.1. Reports unusual findings in MISREPs.

2.2.7.7.3. Helps the Wing/Group WSO/EWO/ECP prepare OCRs.

2.2.7.7.4. Participate in the EWIR action team.

2.2.7.8. The Base or Wing Communications Squadron:

2.2.7.8.1. Ensure DMS offices, base communications centers, and network control centers comply with information processing instructions and develop OIs to provide instructions for handling EW messages and data.

2.2.7.8.2. Participate in the EWIR action team.

2.2.7.8.3. Quickly identifies communications deficiencies affecting EWIR capability to the Wing/Group WSO/EWO/ECP.

2.3. 53d Wing (53d Electronic Warfare Group) and Air Force Special Operations Command Electronic Combat Support Flight (AFSOC/ECSF) Operational Reprogramming Centers: US Air Force maintains operational RCs and support RCs to support both peacetime and wartime EWIR commitments. Operational RCs maintain engineering, operational, and intelligence expertise in the aircraft, mission, and EW systems they support. They are primarily responsible for MD/EID changes and provide expertise and technical support for OFP updates, testing, fielding of new systems, requirement definitions, training, configuration control, etc. Support RCs maintain engineering expertise in most US Air Force EW systems. It also supports the operational RCs during the building and testing of MD/EID changes. WR-ALC maintains an operational RC for FMS (WR-ALC/LNI).

2.3.1. Responsible for all MD development, production, testing, and distributing as well as delegation of these tasks to other agencies, as required. (Exception; MD development for ECISAP customers shall be according to Section 5 of this AFI and the Memorandum Of Agreement on 53 EWG and WR-ALC/LN *Foreign Military Sales Mission Data Programming*, dated 13 Jun 97.)

2.3.2. Provide guidance and technical help with developing intelligence, logistics, and communications systems in support of EWIR.

2.3.3. Maintain software support facilities IAW the EW System Managers' life cycle management plan or LCMP for legacy systems.

2.3.4. Evaluate EW MD and support documentation to maintain configuration control.

2.3.5. Support all operational testing required to fully evaluate all EW software or MD changes.

2.3.6. Create training parameters for EW systems, as necessary.

2.3.7. Identify formal intelligence requirements and submit to MAJCOM/IN.

2.3.8. Maintain a Bulletin Board System (BBS) as a means of distributing reprogramming data.

2.3.9. Conduct force development evaluation to determine system performances and find specific EW system deficiencies.

2.3.10. Prepare SIMs when changes in the threat environment might affect EW systems in the theater.

2.3.11. Submit final software change messages (SCMs) to AFMC.

2.3.12. Evaluate and resolve field Operational Change Requests (OCRs).

2.3.13. Produce and send MIMs when appropriate.

2.3.14. Contribute information to test plans concerning the nature of required tests and independent verification and validation (IV&V).

2.3.15. Develop system handbooks or EC mission guides for each assigned EW system.

2.3.15.1. 53 WG (ACC) and ECSF (AFSOC) update and distribute the handbooks and mission guides when required or concurrently with each MD update.

2.3.16. Participate in reprogramming exercises.

2.3.17. Provide engineering support and tactical expertise to ECISAP as defined in [Chapter 5](#).

- 2.3.18. Contact the appropriate SPCs for threat validation and NSA for collection verification.
- 2.3.19. Provide EW system engineering support for FME testing and analysis to ensure timely system performance assessment is accomplished.
- 2.3.20. Develop and maintain plans and manning to operate 24 hour Emergency RCs in support of contingencies and combat operations or as directed by MAJCOMs or the theater commanders.
- 2.3.21. Inform MAJCOM DO and LG, or their equivalents, of technical data change requirements caused by upcoming PACER WARE updates as soon as practical.
- 2.3.22. Provide AFIWC (453 EWS) with all MD changes to ensure that flagging models are kept current with the appropriate MD.

2.4. Air Force Materiel Command (AFMC) (Reprogramming Center [RC]). AFMC and WR-ALC/LN:

- 2.4.1. Responsible for all Operational Flight Program (OFP) development, production, developmental testing, and distribution, as well as delegation of these tasks to other agencies, as required. Also ensure:
 - 2.4.1.1. Users receive fully developed and tested EW systems and EWIR improvements with the operational capabilities they have specified.
 - 2.4.1.2. All EW systems are rapidly reprogrammable.
 - 2.4.1.3. Each EW system includes these fully tested items, both at the RCs and in the field, at delivery of the first asset:
 - 2.4.1.3.1. Reprogramming support tools (including flagging models, MD generators, hot bench mock-ups, emulators, support computers, and necessary line replaceable units [LRUs]).
 - 2.4.1.3.2. Data transfer equipment (memory loader verifiers [MLVs], Common Aircraft Portable Reprogramming Equipment (CAPRE), enhanced diagnostic aide [EDNA], etc).
 - 2.4.1.3.3. Support equipment (field and depot-level).
 - 2.4.1.3.4. All aspects of software reprogramming and support facilities.
- 2.4.2. Plan, integrate, and acquire new EWIR systems.
- 2.4.3. Identify opportunities for acquiring joint systems.
- 2.4.4. Use the EWIRDB and other sources of information to develop and initiate reprogramming efforts for CAF/MAF/AFSOC EW systems (including all systems supported via IAs or SAPs, based upon FMS agreements).
- 2.4.5. Provide logistics and engineering support for both the hardware and software elements of EW systems and their associated support, training, and range simulator equipment.
- 2.4.6. Establish and manage facilities and personnel to analyze, develop, and test changes to:
 - 2.4.6.1. Operation Flight Program (OFP)
 - 2.4.6.2. EW system support tools
 - 2.4.6.3. Support equipment software

- 2.4.7. Maintain facilities for complete EW system ground testing.
- 2.4.8. Maintain equipment to transmit EW software changes to units worldwide.
- 2.4.9. Respond to approved SCMs.
- 2.4.10. Provide MD support when requested.
- 2.4.11. Identify, obtain, develop, and maintain EW systems software reprogramming tools.
- 2.4.12. Provide data necessary (including parametrics) for AFIWC (453 EWS) to develop and maintain flagging models on systems AFMC manages.
- 2.4.13. Update and maintain a software support plan for each EW system. These plans should be a derivative from each systems life cycle management plan, for legacy systems refer to the LCMP.
- 2.4.14. Chair the Configuration Management Subcommittee (WR-ALC/LNE) and informs HQ USAF/XO of the committee's progress.
- 2.4.15. Provide EW engineering and logistics support to allied and friendly nations through the ECISAP, as detailed in [Chapter 5](#).
- 2.4.16. Notify the appropriate MAJCOM, JFACC/CFACC/AOC of FMS sales of EW equipment (including software updates) that AFMC manages or develops.

2.5. Air Force Operational Test and Evaluation Center (AFOTEC). AFOTEC will work closely with MAJCOMs, system program offices (SPOs) and reprogramming support organizations to:

- 2.5.1. Plan for, conduct, and report on all OT&E IAW AFI 99-102 as required on new or upgraded EW systems and associated reprogramming support equipment.
 - 2.5.1.1. Coordinate OT&E reprogramming requirements with MAJCOMs and the SPOs.
 - 2.5.1.2. Participate in combined DT&E/OT&E and combined test forces (CTF) on EW systems and reprogramming equipment to the maximum extent practical without compromising the independence of the dedicated phase of OT&E.
 - 2.5.1.3. Perform OT&E on EW systems and reprogramming equipment and identify operational impacts, strengths, and weaknesses in EW system effectiveness and suitability to MAJCOMs.
 - 2.5.1.4. Participate in the certification of system readiness for dedicated OT&E according to AFMAN 63-119, and "accept" systems (or reject, as appropriate) for OT&E.
 - 2.5.1.5. Participate in EWIR Committees and subcommittees.

2.6. Air Intelligence Agency (AIA):

- 2.6.1. Develop a guide describing the role of collectors in EW reprogramming analysis.
- 2.6.2. Train both operators and collectors (including crew briefings and debriefings) in intelligence matters.
- 2.6.3. Work with HQ USAF/XOI, NSA, and DIA to ensure supporting IPCs and SPCs:
 - 2.6.3.1. Review operational intelligence requirements to support EWIR.

2.6.3.2. Assess technical and operational SIGINT for validation and reporting (using available intelligence products) to the RCs, Agencies, and MAJCOM/IN.

2.6.3.3. Ensure intelligence collection and production methods exist to provide near real-time assessments of technical and operational ELINT.

2.6.3.4. Identify unsatisfied operational intelligence requirements to support EWIR and report them to:

2.6.3.4.1. HQ USAF/XOI

2.6.3.4.2. Appropriate national intelligence production centers

2.6.3.4.3. Gives theater-collected ELINT intercept and other intelligence data to the RCs, AFIWC, NAF Information Warfare Flight and to the appropriate EWIRDB production centers for timely engineering assessment of threat system capabilities.

2.6.4. Ensure Information Warfare (IW) Flights are well versed in EWIR procedures

2.6.5. The Air Force Information Warfare Center (453 EWS):

2.6.5.1. Serve as the EWIR process expert for the MAJCOM or NAF tasked to support/conduct the Air Force directed reprogramming exercise. As necessary, work with USAF/XOIE and the MAJCOM/NAF to develop:

2.6.5.1.1. Exercise goals and objectives

2.6.5.1.2. Identify EW equipment that will be a part of the reprogramming exercise

2.6.5.1.3. Serve as the focal point for coordination with the JIOC

2.6.5.1.4. Coordinate with RCs and other services, the threat parametric changes that will support the exercise objectives

2.6.5.1.5. Coordinate with SAF/IAF to manage the reprogramming process for FMS countries participating in the exercise

2.6.5.2. Designs, manages, and budgets EW equipment flagging and analysis models.

2.6.5.3. Provides CONUS and in-theater flagging analysis of SIGINT data to the RCs, MAJCOMs, and JFACC/CFACC/AOCs, as required, to support peacetime, exercise, contingency, and wartime operations.

2.6.5.3.1. Identifies threat parameters, which may not be correctly identified by CAF/MAF/AFSOC EW acquisition/analysis systems, RWRs and jammers. Conducts the Air Force flagging program. Models all CAF/AMC/AFSOC EW systems (for signal level and pulse level processing) and identifies emissions which may not be correctly identified by these warning receivers and jammer systems.

2.6.5.3.2. Designs, develops, maintains, and distributes the flagged signals database.

2.6.5.3.3. Provides Flagging Databases for EW systems to identify locations of changed emitters as well as the new emitter operating parametrics.

2.6.5.4. Evaluates PACER WARE actions during wartime and contingency operations, as HQ USAF/XO directs.

2.6.5.5. Produces parametric information on US-produced (or manufactured), owned and operated radar and EW systems. Additionally, produces parametric information on requested rest-of-world (ROW) radar, communications and EW systems.

2.6.5.6. Serve as reachback contingency support for post-event analysis and modeling of radar warning receiver mission-under-duress indications. The 453 EWS will coordinate technical responses with the appropriate reprogramming center (53 EWG/AFSOC/ECSF/AMC).

2.6.5.7. Coordinates with the SPCs for analysis of aircrew and electronic support inputs on threat parameter changes and new threats, if reported parameters are outside EWIRDB assessed limits.

2.6.6. National Air Intelligence Center (NAIC):

2.6.6.1. Serves as DoD executive agent for the EWIRDB, as required by the DIA.

2.6.6.1.1. As the EWIRDB Executive Agent serves as the focal point for all EWIRDB Problem Reports. These are available via the NAIC Website (Top Secret and Secret) under the EWIRDB homepage.

2.6.6.2. Produces the EWIRDB product by merging data from NAIC analysis, with data from other SPCs, the NSA (for Kilting ELINT data), and AFIWC (for US and requested ROW data).

2.6.6.3. Distributes and provides on-line access to the EWIRDB.

2.6.6.4. Performs administrative checks on the EWIRDB inputs to confirm the data is correctly formatted.

2.6.6.5. Updates parametric information on assigned foreign aerospace threat systems, ground-based early warning/acquisition radar threat, and hostile command and control (C2) or IW systems for the EWIRDB.

2.6.6.6. Provides consumers with EWIRDB data for reprogramming during exercise, contingency, and wartime operations.

2.6.6.7. Coordinates with AFMC and SAF/AQ to provide equipment and support for ground and airborne testing against foreign assets.

2.6.6.8. Assists the RCs' participation in FME.

2.6.6.9. Produces tailored EWIRDB products to support FMS threat data requirements by pulling data from the EWIRDB.

2.6.6.10. Provides a representative to serve on all EWIR committees as the interface to both the Intelligence community and the EWIRDB program.

2.6.6.11. Ensures Rivet Joint and Combat Sent data is made available to the RCs and flagging.

2.6.6.12. Produces and maintains the Airborne Systems Database (ASDB) containing the official DoD "electronic fit list" of threat airborne platforms.

2.7. Air Force Air Operations Center (AOC). These procedures apply to the US Air Force component of the Joint Forces Air Component Commander (JFACC) and Combined Forces Air Component Commander CFACC. The AOC is the operations center of the CAF/MAF Commander. Within the AOC, threat evaluation and identification of changing target/mission requirements are continuous and time-critical functions. The AOC:

- 2.7.1. Monitors the EW threat environment in the AOR.
- 2.7.2. Performs preliminary operational deficiency analysis, generates, and sends field OCRs to the MAJCOMs and RCs.
- 2.7.3. Take action to minimize the impact of threat changes to increase aircraft survivability. This action includes, but is not limited to:
 - 2.7.3.1. Notifying aircrews of loss or degradation of EW capability
 - 2.7.3.2. Use new tactics
 - 2.7.3.3. Avoiding certain threat areas (if feasible)
 - 2.7.3.4. Divert attack forces to other targets
 - 2.7.3.5. Use Suppression of Enemy Air Defenses (SEAD) assets
 - 2.7.3.6. Review SIM recommendations
- 2.7.4. Distributes reprogramming change information to joint and combined organizations to ensure interoperability and avoid EW frequency conflicts.
- 2.7.5. Report friendly force anomalies leading to false identifications or inappropriate responses and request supporting IPCs, RCs and EWIRDB production centers validate these anomalies.
- 2.7.6. Review Operational reports (OPREP), mission reports (MISREP), EWIR messages and flight reports (FLTREP). Analyze these reports and messages to find:
 - 2.7.6.1. Unusual EW equipment operation
 - 2.7.6.2. Changes in engagement tactics
 - 2.7.6.3. Changes in successful engagement rates
 - 2.7.6.4. Ensure that theater MISREPs are sent to supporting RCs and AFIWC (453 EWS).
- 2.7.7. Ensures units deployed to their theater have the capability to quickly receive and upload reprogramming data.
- 2.7.8. Ensures deployed units have all required equipment to perform rapid reprogramming, to include EW support equipment (e.g., Program Loader Verifiers (PLVs)/Memory Loader Verifier (MLVs), Digital Computer System (DCS'), BBS equipment, CAPRE, mission support facilities, etc.).
- 2.7.9. As delegated by the JFACC/CFACC, coordinates and implements software changes from the RCs for its combat units, depending on:
 - 2.7.9.1. Its assessment of the change
 - 2.7.9.2. Nature and lethality of the threat change
 - 2.7.9.3. Planned force movement
 - 2.7.9.4. Critical timing

2.8. EWIR Committee and Subcommittee Interoperability:

2.8.1. Oversight Committee. HQ USAF/XOIE chairs the Oversight Committee and performs the following duties:

2.8.1.1. Defines and manages the EWIR process.

2.8.1.2. Reviews sub-committee actions and resolves identified problems.

2.8.1.3. Notifies applicable DOD agencies of EWIR requirements. Works with other services to seek areas of commonality, ensure interoperability, and minimize duplication.

2.8.1.4. Calls a meeting of the Oversight Committee at least annually, or when required.

2.8.2. EWIR Subcommittees . EWIR subcommittees help maintain and improve effective world-wide EWIR and perform the following duties:

2.8.2.1. Comply with the directives in EWIR-related PMDs, including the EWASIF PMD.

2.8.2.2. Hold meetings to discuss and resolve issues. Schedule meetings as the sub-committee chairperson, the membership or the Oversight Committee chairperson requests.

2.8.2.3. Write and distribute subcommittee charters and meeting minutes.

2.8.3. Reprogramming Center Support Subcommittee . AFMC (WR-ALC/LNE) chairs this sub-committee, which:

2.8.3.1. Develops and integrates common support software and hardware.

2.8.3.2. Reviews EWASIF funding and recommends priorities to HQ USAF/XOIO.

2.8.3.3. Reviews RC system software and reprogramming support tools requirements and recommends funding priorities

2.8.4. Communications Requirements Subcommittee . 68 EWS/EWP chairs this subcommittee which:

2.8.4.1. Ensures new and existing reprogramming support equipment will support EWIR.

2.8.4.2. Ensures communications capability will adequately support current and future connectivity to common users, base-level, and long-haul systems. Focuses on requirements to drive recommended technical solutions for communications connectivity between RCs, AFIWC, intelligence support agencies, MAJCOMs, JFACC/CFACC/AOCs, and the Wings/Groups.

NOTES:

1. The EWIR Oversight Committee Chairperson approves subcommittee charters.
2. A complete membership list is provided at [Attachment 2](#).

Chapter 3

OPERATIONAL PROCEDURES

3.1. EWIR Deficiency Reporting. Organizations and individuals performing EWIR must identify EW deficiencies via the operational change request (OCR) (see [Attachment 4](#)).

3.1.1. EW deficiencies may come from:

- 3.1.1.1. New threats
- 3.1.1.2. Changed parameters of existing threats
- 3.1.1.3. Aircrew or maintenance personnel interested in improving system operation
- 3.1.1.4. Changes in operational environment
- 3.1.1.5. Changes in the intended use of the EW equipment

3.1.2. OCR Process:

- 3.1.2.1. The wing or group WSO/EWO/ECP or RC sends the OCR to their MAJCOM and/or JFACC/CFACC/AOC with an informational copy to the appropriate operational RC.
- 3.1.2.2. The MAJCOM, CFACC/JFACC/AOC, and RC prioritize and evaluate the OCR and suggest methods for implementing it.
- 3.1.2.3. The operational RC may send an SCM to the supporting RC when the OCR affects the OFF, EW system hardware, etc.

3.1.3. Prioritizing OCRs. The OCR originator prioritizes OCRs using these designators:

- 3.1.3.1. E (Emergency)
- 3.1.3.2. U (Urgent)
- 3.1.3.3. R (Routine)

3.1.4. Originators submit emergency OCR messages with an IMMEDIATE precedence:

- 3.1.4.1. To change operational characteristics that might seriously threaten national security
- 3.1.4.2. When a condition exists preventing an adequate response to a threat, and the situation warrants immediate action
- 3.1.4.3. To change operational characteristics that might result in fatal or serious injury or extensive equipment damage or destruction

3.1.5. Emergency changes are worked, to the exclusion of all other activities, by the RCs on a 24-hour basis until complete.

3.1.6. Originators submit urgent OCR messages with a ROUTINE precedence:

- 3.1.6.1. To change operational characteristics that might seriously threaten mission effectiveness
- 3.1.6.2. When a condition exists preventing an adequate response to threat-associated system, and the situation is normal but warrants immediate action
- 3.1.6.3. To change operational characteristics that might result in injury or equipment damage

3.1.7. Urgent changes are worked, to the exclusion of all other activities, by the RCs full-time during normal duty or extended duty hours, with a completion goal of 10 days. These changes take precedence over any other activity except emergency changes.

3.1.8. Originators submit routine OCR messages with a ROUTINE precedence when:

3.1.8.1. The system has a high probability of correctly responding to a threat or can compensate for threat and friendly emitter changes but minor deficiencies exist that may show an error.

3.1.8.2. The situation is normal and does not warrant immediate action.

3.1.8.3. The deficiencies or errors are not a hazard to personnel or equipment.

3.1.8.4. Changes in training MD are desired.

3.1.9. Routine OCRs are normally scheduled and included in block cycle updates for the affected EW equipment.

3.1.10. The priority of the OCR will be included in the text of the message.

3.2. Implementing Changes. When the MAJCOM or JFACC/CFACC/AOC directs, units load software reprogramming changes to CC (combat) coded aircraft. With Wing/CC (or designated representative) approval, units will schedule and upload software changes on TF (training) and CB (test) coded aircraft as soon as possible, on a non-interference basis with programmed training and testing.

3.2.1. Messages. EWIR messages and data are normally sent in the order listed below. However, many factors enter into when an agency or unit receives these messages and in what order they are received. These factors include, but are not limited to:

3.2.1.1. Priority of the change(s)

3.2.1.2. Location of the originator

3.2.1.3. Common-user messaging system traffic congestion

3.2.1.4. Unit distribution policies

3.2.1.5. Whether or not the unit has BBS capability

3.2.1.6. SIM. Usually the first time a unit knows a threat change has occurred. Unit may receive one SIM followed shortly by the RIM, MIM or TCTO, DAT, and IMP for a particular EW system. Or, it may receive a number of SIMs affecting a particular EW system, over a period of time, before the RIM, MIM or TCTO, DAT, and IMP for that system is received.

3.2.1.7. RIM, MIM or TCTO, and DAT. During emergency or high priority software changes, these messages are usually coordinated to be sent at approximately the same time. Due to the factors described above, the actual order the unit receives them may vary. For routine changes, the order and time elapsed between may vary widely from days, to weeks, to even months.

3.2.1.8. IMP. During emergency or high priority software changes, the unit can expect to receive the IMP nearly simultaneous with, or shortly after, the above messages. For routine changes, the IMP may not be received for days, weeks, or even months.

3.2.2. EWIR message descriptions.

3.2.2.1. Flagging Report (FLR). AFIWC (453 EWS) sends FLRs to the RCs, MAJCOM and JFACC/CFACC/AOC, and other agencies when requested (see [Attachment 3](#)).

3.2.2.1.1. Intelligence data is processed through CAF/MAF/AFSOC EW system models that predict system responses.

3.2.2.1.2. Details of incorrect responses and the corresponding intelligence data are reported via the FLRs.

3.2.2.1.3. Provides an early indication of potential problems.

3.2.2.2. System Impact Message (SIM). The appropriate RC sends the SIM to the units and MAJCOM or JFACC/CFACC/AOC (see [Attachment 6](#)). This message:

3.2.2.2.1. Describes the impact of threat changes on an EW system.

3.2.2.2.2. Discusses system deficiencies.

3.2.2.2.3. Recommends interim corrections (e.g., interim tactics, recommended employment options, etc.).

3.2.2.3. Reprogramming Impact Message (RIM). The appropriate RC sends the RIM to units and MAJCOM or JFACC/CFACC/AOC (see [Attachment 7](#)). This message:

3.2.2.3.1. Describes in detail how an EWIR change affects an EW system.

3.2.2.3.2. States the impact of implementing or not implementing the change.

3.2.2.3.3. Helps aircrews and commanders decide when or whether to implement a change.

3.2.2.4. Maintenance Instruction Message (MIM). The appropriate RC sends the MIM, which provides maintenance uploading instructions, to units along with the changes for an EW system (see [Attachment 8](#)).

3.2.2.5. Time Compliance Technical Order (TCTO). The appropriate ALC (in most cases, WR-ALC) sends the TCTO to units (see [Attachment 9](#)). This message includes information on:

3.2.2.5.1. New Block Cycle or operational flight program (OFP)

3.2.2.5.2. Changes to system Handbooks or Mission Guides

3.2.2.5.3. Changes to mission data

3.2.2.5.4. Implementation instructions

3.2.2.6. Implementation Message (IMP). The MAJCOM or JFACC/CFACC/AOC prepares the IMP, which notifies units to upload a specific EW software change (see [Attachment 10](#)). This message may also include timing criteria and notification instructions. The IMP is also sent to the RCs to notify them of the status of the change.

3.2.2.7. Unit Loading Message (ULM). Units send the ULM to the MAJCOM or JFACC/CFACC/AOC and appropriate RCs after the units have finished uploading EW software change to all available aircraft (actual); or when the number of systems has been uploaded as instructed by the implementing authority (exercise) (see [Attachment 11](#)).

3.2.2.7.1. Send the ULM within 3 duty days after completion of any reprogramming activity. Units report the following information to the MAJCOM or JFACC/CFACC/AOC, RCs, and

other appropriate addressees. (**NOTE:** Actual addressees are normally identified by the MAJCOM in their IMP for each software change):

- 3.2.2.7.1.1. A synopsis of reprogramming changes, including start and stop times for each reprogramming action
- 3.2.2.7.1.2. Any problems a unit encountered
- 3.2.2.7.1.3. Any MAJCOM specific instructions
- 3.2.2.7.1.4. These reporting requirements are exempt from Report Control Symbol (RCS) licensing in accordance with AFI 33-324, *Management and Control of Information Reports Requirements*.

NOTES:

1. Classification of ULMs is IAW individual system or aircraft classification guide.
2. Addressees for ULMs are normally provided by the implementation authority in the IMP message(s).

3.2.2.8. Status Message (STM). Are sent by the RCs to the units, MAJCOMs, the JFACC/CFACC/AOC, and any other interested parties, during periods of heightened activity or exercises (see [Attachment 12](#)). This message provides updates of current reprogramming actions, to include estimated time of completion. Send the STM every 72 hours, or as requested by the lead MAJCOM, throughout the period of activity or exercise.

3.2.2.9. Semi-Annual EWIR Summary. Are sent by the RCs to the units, MAJCOMs, and any other interested parties. It summarizes the current software configurations of the particular EW systems, software loads currently available (by theater, if applicable), status of all outstanding SIMs, and status of ongoing reprogramming actions. This Summary should be made available both in hard copy and on the BBS.

3.2.2.10. Threat Change Validation Request (TCVR). The appropriate RC sends a TCVR to the appropriate SPC regarding collected parameters that would require a significant change to the information already known about a threat system. This message contains information concerning the system and parameters in question and a detailed report of what validation is necessary. The TCVR is a request to validate a threat change or to declare it invalid.

3.2.2.11. Threat Change Validation Message (TCVM). Are sent by SPCs to the appropriate RCs to initiate Reprogramming Actions. After receiving the TCVR, the analysts at the SPC will make a technical assessment whether the parameters in question are a true capability and/or mode of the threat system, and sends a TCVM if the threat is valid.

3.3. Timeliness of Reprogramming Actions. All reprogramming messages (e.g., TCVM, FLR, SIM, OCR, RIM, MIM, TCTO, DAT, IMP, etc.) will include either a ROUTINE or IMMEDIATE precedence in the subject line. Recipients (SPCs, RCs, MAJCOMs and flying units) of reprogramming messages will perform reprogramming actions, if required, based upon the precedence of the message. **NOTE:** Precedence may change if a crisis occurs, or ends, in the middle of specific reprogramming action. Use the following criteria when performing reprogramming actions (see paragraph [3.2](#) for exceptions):

3.3.1. ROUTINE. Treat reprogramming actions as normal day-to-day operations. Flying units may schedule around the daily training/maintenance schedule. **NOTE:** A not later than date (NLT) for completion may be given by the implementation authority.

3.3.2. IMMEDIATE. Treat as an emergency reprogramming action. Immediately perform reprogramming actions as required by the reprogramming message. Flying unit commanders may determine if training or operational missions can or cannot be flown without reprogramming actions being performed. **NOTE:** During all exercises, MAJCOM/IG timelines are used to determine flying units success in meeting IMMEDIATE timeliness.

Chapter 4

EXERCISES AND EVALUATION PROGRAMS

4.1. General.

4.1.1. The Air Force must evaluate its EW reprogramming by conducting reprogramming exercises periodically to:

4.1.1.1. Identify problem areas

4.1.1.2. Gain confidence

4.1.1.3. Ensure a smooth flow of information during a crisis

4.1.1.4. Ensure readiness in response to threat parameter changes

4.1.1.5. Train operations, intelligence, communications, and maintenance personnel

4.1.2. Reprogramming Exercises. Exercises should be held with joint exercises to the maximum extent possible. Joint exercises expose all levels of the EWIR process to communications limitations inherent in large scale exercises and test joint coordination and cooperation between the services. Joint exercises may include FMS participation.

4.1.3. Exercise Categories. Exercises fall into three categories:

4.1.3.1. Air Force directed

4.1.3.2. MAJCOM directed

4.1.3.3. Local

4.2. Air Force Directed Exercises.

4.2.1. These exercises:

4.2.1.1. Normally cover the entire EWIR process.

4.2.1.2. Duplicates to the largest extent possible real world operations. Reduce artificiality of the exercise to the absolute minimum.

4.2.1.3. May include FMS participants.

4.2.2. Document the capabilities and limitations of all major components of reprogramming, including:

4.2.2.1. Collecting, validating, and distributing intelligence information.

4.2.2.2. Evaluating signals

4.2.2.3. Creating and testing changes

4.2.2.4. Distributing changes

4.2.2.5. Implementing changes

4.2.2.6. Validating equipment changes in combat units

4.2.3. May be suspended by HQ USAF/XO due to recent significant world events, which demonstrated successful reprogramming capability to a majority of US Air Force EW systems.

4.3. MAJCOM Directed Exercises.

4.3.1. These exercises:

4.3.1.1. Focus on MAJCOM-selected aspects of reprogramming.

4.3.1.2. Usually validate the procedures for distributing emergency reprogramming data to units.

4.3.1.3. Identify shortcomings in communications and support equipment.

4.3.1.4. Will not be held within one month of the AF exercise or within the same quarter. (The AF exercise serves as a MAJCOM exercise.)

4.3.2. Unit Participation. Periodic exercise participation is at the unit Commander's discretion. If the unit Commander chooses not to participate, report reason for non-participation. Reasons may include: unit deployment, IG visit, unit stand-down, etc.

4.3.3. May be suspended by the MAJCOM due to significant world events, or a recent demonstration of successful reprogramming capability to the majority of the MAJCOM's EW systems.

4.4. Local Exercises.

4.4.1. Wing/Groups may:

4.4.1.1. Set up exercises to give personnel a chance to practice reprogramming. **NOTE:** Higher headquarters may also set up such exercises.

4.4.1.2. Decide to conduct limited, periodic reprogramming exercises after reviewing exercise results.

4.4.2. Wing/Groups should coordinate with their MAJCOM and appropriate RCs for availability of exercise data and messages.

4.4.3. EWIR messages and data may be sent to the unit over common-user messaging system or be made available on the BBS, as time and taskings permit.

Chapter 5

INTERNATIONAL AGREEMENTS AND SECURITY ASSISTANCE

5.1. Purpose. EWIR supports EW programs with allied and friendly air forces through various agreements and security assistance programs. The purpose is to foster a greater combined war capability.

5.2. Scope. The two basic areas of EWIR support are international agreements and security assistance programs.

5.2.1. International Agreements. These agreements may:

5.2.1.1. Take several forms (i.e., cooperative research or data exchange agreements, joint development programs, joint exercises, etc.).

5.2.1.2. Require EWIR support to enhance or maintain their effectiveness.

5.2.2. Security Assistance Programs. These agreements:

5.2.2.1. Take the form of FMS agreements.

5.2.2.2. Represent the majority of EWIR supported programs with allied and friendly nations.

5.2.2.3. Electronic Combat International Security Assistance Program (ECISAP) is an AF concept that manages the EC aspects of most FMS agreements.

5.3. Objectives. EWIR support of allied and friendly nations follows the US Air Force EWIR process with the exception of release approval. Procedures, actions, and organizational responsibilities outlined in [Chapter 2](#), [Chapter 3](#), [Chapter 4](#), and this chapter form the basis for EWIR support of international agreements and security assistance programs. FMS software support processes will mirror the USAF support processes where feasible. Exceptions require SAF/IAW and HQ USAF/XOIE approval and will be detailed in a MOA.

5.3.1. Allied and friendly nations receive EW system hardware and software that:

5.3.1.1. Well-trained personnel fully support (including US Government [USG] technical support) and maintain.

5.3.1.2. Undergoes testing and documenting according to US Air Force standards.

5.4. Special Factors. Transferring US Air Force military capability to foreign nations and managing EW programs with them involve these special factors:

5.4.1. Contractual Relations. International agreements and security assistance programs are generally contractual in nature. Program changes that require altering supporting documents (i.e., Memorandums of Understanding, FMS case, bilateral or multilateral agreement, etc.) may require the foreign nation to agree to the change.

5.4.2. Funding. Foreign nations must fund FMS programs at no cost to the US Government.

5.4.2.1. Both the United States and the foreign nation normally fund programs based on international agreements.

5.4.3. Disclosure. The transfer of US military information to a foreign nation must take place in accordance with National Disclosure Policy. EW military information includes:

- 5.4.3.1. Deliverable hardware/software
- 5.4.3.2. Technical orders
- 5.4.3.3. Operating manuals
- 5.4.3.4. Employment considerations
- 5.4.3.5. Training
- 5.4.3.6. Threat/training databases
- 5.4.3.7. Deliverable MD and applicable documentation (handbooks/annexes)

5.5. EW Systems Support

5.5.1. USAF Inventory Systems:

5.5.1.1. 53 WG is responsible for MD and coordinates it with WR-ALC/LNI (International Logistics Division) before delivering it to each nation. Primary implementation details will be outlined in a MOA. The following represents two categories of exceptions:

5.5.1.2. Responsibility: Organizational responsibility exceptions will be outlined in a MOA between the 53 EWG and WR-ALC/LN (reference para [5.3.](#)).

5.5.1.3. Procedural: Under emergency reprogramming conditions, the responsible organization delivers the MD to the nation and coordinates the delivery concurrent with other applicable organizations.

5.5.1.4. ECISAP supports USAF EW systems retired from the inventory (mature non-inventory) to the maximum extent possible, although the foreign nation entirely funds this support. (See [5.8.2.](#) for details of program)

5.5.1.5. AFSOC/ECSF will coordinate with WR-ALC/LNI for new agreements when implementation of system reflects SOF or MAF operational inventory.

5.5.2. Non-USAF Inventory Systems:

5.5.2.1. ECISAP generally does not support:

- 5.5.2.1.1. EW systems in DoD inventory but not in the USAF inventory

5.6. Programs.

5.6.1. Established Programs: Established EW programs are being supported by the appropriate RC or are transitioning IAW MOAs as required.

5.6.2. Future Programs . Programs involving future USAF EW systems must be established IAW [Chapter 2](#) and this chapter.

5.7. Functional Responsibilities. Responsibilities follow [Chapter 2](#). These additional specific responsibilities cover EWIR support of allied and friendly air force programs.

5.7.1. Secretary of the Air Force:

5.7.1.1. The Deputy Assistant Secretary of the Air Force for Acquisition Programs (SAF/AQ) coordinates system acquisition for the US Air Force and foreign nations.

5.7.1.2. Within SAF/AQ, the Common Systems Division (SAF/AQPS) oversees EW systems acquisition.

5.7.1.3. The Armaments Cooperation Division (SAF/IAQ) negotiates non-FMS agreements, i.e., cooperative development, data exchange, etc.

5.7.1.4. The Deputy Under Secretary of the Air Force for International Programs (SAF/IA) oversees security assistance policy and program execution.

5.7.1.5. The Disclosure Division (SAF/IAD) establishes and implements the US Air Force disclosure of military information to foreign nations. This implementation takes place according to:

5.7.1.5.1. AFIs covering disclosure.

5.7.1.5.2. A program's Delegation of Disclosure Authorization Letters (DDL).

5.7.1.5.3. Foreign disclosure guidance on EW-related matters.

5.7.1.6. The Weapons Division (SAF/IAW) co-chairs the FMS ECWG and provides:

5.7.1.6.1. Management

5.7.1.6.2. Weapon system expertise

5.7.1.6.3. Oversight management for ECISAP

5.7.1.6.4. Foreign release guidance on EW-related matters

5.7.1.6.5. OPR for the Electronic Warfare Baseline for Foreign Sales

5.7.1.6.6. Coordinate on release of PACER WARE and Serene Byte MD to friendly and allied forces, and maintains 24 hour coordination response channels with RCs and HQ USAF/XOIE

5.7.2. HQ USAF:

5.7.2.1. The Deputy Chief of Staff for Air and Space Operations (HQ USAF/XO) oversees EW operations.

5.7.2.2. Within HQ USAF/XO, two offices are responsible for overseeing ECISAP operations. The Electronic Warfare Division (HQ USAF/XOIE) oversees ECISAP EW operations and co-chairs the FMS ECWG. The Force Development Plans Division (HQ USAF/XOIIA) oversees ECISAP emitter data.

5.7.2.3. HQ USAF/XOIE will:

5.7.2.3.1. Coordinate on release of EW systems and reviews the operational impact and sensitivity of EW programs, information, and technology being transferred to allies and friendly nations.

5.7.2.3.2. Provide security assistance program implementation recommendations to address protection of US operational capabilities/vulnerabilities/limitations and to ensure US-allied interoperability.

5.7.2.3.3. Provide findings for incorporation into the Electronic Warfare Baseline for Foreign Sales and provides recommendations for other DoD policy governing EW capabilities disclosure.

5.7.2.3.4. Will be responsible for resolving MOA issues in conjunction with SAF/IAW.

5.7.2.3.5. Function as the OPR for the release of PACER WARE and Serene Byte MD to friendly and allied forces

5.7.2.3.6. Extend invitations and approves foreign participation in Serene Byte

5.7.2.3.7. Maintain 24 hour communications channels with RCs for emergency response and release staffing.

5.7.2.4. HQ USAF/XOIIA will:

5.7.2.4.1. Review intelligence impact of FMS EW programs.

5.7.2.4.2. Review and respond to requests for US-owned parametric information on a routine, urgent, or emergency basis with timelines established for routine, urgent, and emergency data dissemination.

5.7.2.4.3. Obtain appropriate disclosure guidance on release of emitter data.

5.7.2.4.4. Ensure the resulting database is delivered to the organization that needs it to support system design and programming.

5.7.2.4.5. Participate in ECWG and ECISAP meetings.

5.7.2.4.6. Maintains 24 hour communications channel with RCs for emergency response.

5.7.3. Air Combat Command:

5.7.3.1. The Director of Operations (ACC/DO) oversees combined operations and security assistance programs.

5.7.3.2. The **Conventional Operations and Training** (ACC/DOS):

5.7.3.2.1. Monitors security assistance programs, to include EW systems.

5.7.3.2.2. Acts as the ACC foreign disclosure policy office.

5.7.3.2.3. Participates in ECWG and ECISAP meetings.

5.7.3.2.4. Monitors foreign participation in SERENE BYTE exercises if required.

5.7.3.2.5. Acts as the ACC focal point for ECISAP issues concerning ACC.

5.7.3.2.6. Tasks ACC subordinate units to support FMS cases.

5.7.3.3. The 53 EWG is the Air Force FMS RC responsible for operational MD to the extent specified in MOAs. 53 EWG:

5.7.3.3.1. Coordinates with WR-ALC and the appropriate agencies to ensure customers receive prompt MD support.

5.7.3.3.2. Resolves MD problems for assigned systems.

5.7.3.3.3. Develops operational employment considerations for FMS customers.

5.7.3.3.4. Conducts force development evaluation for ECISAP as required.

5.7.3.3.5. Coordinates on FMS country Computer Resources Life Cycle Management Plans (CRLCMPs).

5.7.3.3.6. Provides weapons systems expertise.

5.7.4. Air Force Materiel Command:

5.7.4.1. The Air Force Security Assistance Center (AFSAC) manages a broad array of security assistance programs, including:

5.7.4.1.1. EW system acquisition

5.7.4.1.2. Logistics support

5.7.4.2. The Aeronautical Systems Center (ASC) provides:

5.7.4.2.1. EW system planning

5.7.4.2.2. Acquisition

5.7.4.2.3. Weapon system expertise

5.7.4.3. The EC Product Group Manager (PGM) plans, develops, acquires, produces, and integrates EW systems.

5.7.4.3.1. The cognizant system program office provides OFP support for systems retained under its control.

5.7.4.4. The EC PGM provides system management and logistics support for most US Air Force EW systems.

5.7.4.5. The EC PGM is the AFMC single manager that provides system management and logistics support, including software and hardware for assigned EW systems.

5.7.4.6. The International Logistics Division (WR-ALC/LNI) manages security assistance for assigned EW programs. The International Logistics Division is an AF FMS RC with the following development and sustainment responsibilities:

5.7.4.6.1. OFP

5.7.4.6.2. MD as required by MOA

5.7.4.6.3. Reprogramming tools

5.7.4.6.4. Test software

5.7.4.6.5. Providing hardware and software configuration control for systems managed by WR ALC/LNI.

5.7.4.6.6. Setting up communication links

5.7.4.6.7. Coordinating block cycle/software changes

5.7.4.6.8. Distributing EW products

5.7.4.6.9. Obtains and submits P&A from all applicable organizations

5.7.4.6.10. Participates in reprogramming exercises.

5.7.4.6.11. Provides CRLCMP for FMS

5.7.4.6.12. Provides country specific system security classification guides.

5.7.4.7. Ogden Air Logistics Center (OO-ALC) programs aircrew training and range simulators. Unit Training Devices (UTDs) are reprogrammed by the responsible ALC.

5.7.4.8. Ogden Air Logistics Center (OO-ALC) programs training range simulators.

5.7.4.9. Oklahoma City Air Logistics Center (OC-ALC) programs the E-3's Electronic Support Measures (ESM) system.

5.7.4.10. Air Armament Center (AAC) develops, acquires, and sustains aerial targets and ranges and their related electronic warfare (EW) payload systems to test and evaluate weapon systems and conduct realistic operational training. In addition, the AAC operates the Multi-Spectral Test and Training Environment range at Eglin AFB and provides development testing to allied and foreign nations.

5.7.4.11. AFSAC/IPD manages AFMC's disclosure of military information to foreign nations. *NOTE:* Each ALC also has an office that helps with that ALC's programs.

5.7.5. Air Intelligence Agency (AIA):

5.7.5.1. The National Air Intelligence Center (NAIC):

5.7.5.1.1. Provides support to AF/XOI and SAF/IA on foreign technological capabilities for comparison with US EW systems capabilities in support of disclosure decisions.

5.7.5.1.2. Develops and maintains the software responsible for releasing properly coded EWIRDB information for FMS release.

5.7.5.1.3. Generates and distributes FMS-releasable EWIRDB products when required by FMS production schedule and when requested by AF/XOIIA to support program requirements.

5.7.5.1.4. Delivers these products to RCs

5.7.5.2. The Air Force Information Warfare Center (AFIWC):

5.7.5.2.1. AFIWC (453 EWS) provides US systems data for release when required by FMS production schedule.

5.7.5.2.2. Provides support to HQ USAF/XO for developing operational assessments in support of EW capability disclosure.

5.8. US Air Force Management:

5.8.1. FMS EC Working Group (ECWG). The FMS ECWG, develops, recommends policy for and oversees the export of US Air Force EW systems and system support.

5.8.1.1. FMS ECWG policy recommendations will be forwarded to the Air Staff and Secretariat for approval and will be incorporated in the Air Force EW Baseline for Foreign Sales or other Air Force policy as appropriate.

5.8.1.2. HQ USAF/XOIE and SAF/IAW co-chair the FMS ECWG.

5.8.1.3. Additional members come from:

5.8.1.3.1. SAF

5.8.1.3.2. HQ USAF

5.8.1.3.3. HQ ACC/DOTS

5.8.1.4. Nonvoting members that provide technical support to the FMS ECWG are:

5.8.1.4.1. AIA

5.8.1.4.2. 53 EWG

5.8.1.4.3. WR-ALC/LNI

5.8.1.4.4. Other MAJCOM support agencies involved in the export of US Air Force EW systems, support equipment, and systems support

5.8.2. Electronic Combat International Security Assistance Program (ECISAP). ECISAP provides acquisition, logistics, technical engineering, and training services to ensure the effectiveness of EW systems the US Air Force sells to allied and friendly nations. This support program provides the standardization and dependability that participating ECISAP member nations need to field effective EW systems.

5.8.2.1. ECISAP acts IAW:

5.8.2.1.1. National Disclosure Policy

5.8.2.1.2. US Air Force manuals (e.g. AFMAN 16-101)

5.8.2.1.3. FMS ECWG direction

5.8.2.1.4. The terms of each FMS program

5.8.2.1.5. Electronic Warfare Baseline for Foreign Sales

5.8.2.1.6. Applicable Delegation of Disclosure Letters (DDLs)

5.8.2.2. WR-ALC/LNI is the ECISAP Executive Agent. The Executive Agent will:

5.8.2.2.1. Obtain and submit pricing and availability (P&A) for ECISAP programs

5.8.2.2.2. Develop and coordinate database delivery schedules

5.8.2.2.3. Be the OPR for organizing ECISAP meetings/activities

5.8.2.2.4. Assist SAF/IA with program management activities

5.8.2.3. The key ECISAP administering agencies are:

5.8.2.3.1. AF/XOIE

5.8.2.3.2. SAF/IAWS

5.8.2.3.3. ACC/XOSF

5.8.2.3.4. Air Force Security Assistance Center (AFSAC)

5.8.2.3.5. Air Force Security Assistance Training (AFSAT)

5.8.2.3.6. AF/XOIIA

5.8.2.4. The ECISAP implementing agencies are:

5.8.2.4.1. NAIC

5.8.2.4.2. WR-ALC/LNI

5.8.2.4.3. 53 EWG

5.8.3. Additional EWIR-Supported Programs:

5.8.3.1. Air Force directed reprogramming exercises may include allied and friendly nations to demonstrate US Air Force support and provide training.

5.9. Operational Procedures. Each nation's CRLCMP contains procedures that detail such actions as block cycle responsibilities.

5.10. Intelligence. AF/XOIIA provides the necessary emitter data for producing and maintaining EW software and operational considerations. Its primary product is the country-specific EWIRDB, which NAIC produces with input from the AFIWC and appropriate US intelligence community agencies.

5.11. Communications.

5.11.1. US Air Force EWIR communication procedures form the basis for deliveries to foreign nations.

5.11.2. The ECISAP RCs maintain a secure communications and a BBS capability (see country and system CRLCMP for details). These links provide the necessary connectivity for transmitting text and binary data between the RCs and foreign nations.

5.11.3. Security of International Transmissions. NSA ensures the establishment of secure transmission channels for the physical transfer of documents and software or the electronic transfer of data and documentation.

NOTE: Electronic transmission is the desired method.

5.11.3.1. USG personnel supporting FMS countries may receive and transmit reprogramming software and messages via the BBS or STUs.

5.12. Support. ECISAP operational, technical, training and logistics support comes primarily from the following agencies:

5.12.1. 53 EWG provides MD and operational considerations for foreign use of US Air Force EW equipment.

5.12.2. AFSOC/ECSF provides MD and operations considerations for system similar to SOF and MAF configured EW equipment.

5.12.3. WR-ALC/LNI provides contracting, technical assistance, logistics support, and hardware and software configuration control for assigned systems.

5.12.4. ACC Mobile Training Teams (MTTs) are available (non-interference basis) for in-country instruction on EW subjects, EW pod operations, and operational considerations, when requested by the foreign government.

5.12.5. NAIC provides FMS databases.

5.12.6. AFSAT develops and provides FMS training plans.

ROBERT H. FOGLESONG, Lt General, USAF
Deputy Chief of Staff , Air & Space Operations

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

ACC—Air Combat Command

AETC—Air Education and Training Command

AFDTC—Air Force Developmental Test Center

AFIWC—Air Force Information Warfare Center

AFMC—Air Force Materiel Command

AFOTEC—Air Force Operational Test and Evaluation Center

AFRC—Air Force Reserve Command

AFSAC—Air Force Security Assistance Center

AFSAT—Air Force Security Assistance Training

AFSOC—Air Force Special Operations Command

AIA—Air Intelligence Agency

ALC—Air Logistics Center

ALIC—Air Launcher Interface Computer

AMC—Air Mobility Command

AOC—Air Operations Center

AOR—Area of Responsibility

ARC—Air Reserve Component (USAFR and ANG)

ASC—Aeronautical Systems Center

ATS—Automatic Test Station

AUTODIN—Automatic Digital Network

BBS—Bulletin Board System

C2—Command and Control

CAF—Combat Air Forces

CAPRE—Common Aircraft Portable Reprogramming Equipment* (Note: Will replace DCS and MLVs/PLVs when fielding is complete)

CFACC—Combined Force Air Component Command

CID—Combat Intelligence Division

COMSEC—Communications Security

ConPlan—Contingency Plan

CRLCMP—Computer Resources Life Cycle Management Plan
CRWG—Computer Resource Working Group
DCS—Digital Computer System
DDL—Delegated Disclosure Letters
DIA—Defense Intelligence Agency
DISN—Defense Information Systems Network
DSSCS—Defense Special Security Communications Systems
DMS—Defense Message System
EA—Electronic Attack
EC—Electronic Combat
ECISAP—Electronic Combat International Security Assistance Program
ECP—Electronic Combat Pilot
EC PGM—Electronic Combat Product Group Manager
ECWG—Electronic Combat Working Group
EDNA—Enhanced Diagnostic Aid
EID—Emitter Identification Data
ELINT—Electronic Intelligence
ERC—Emergency Reprogramming Center
EOB—Electronic Order of Battle
ES—Electronic Support
ESM—Electronic Support Measures
EW—Electronic Warfare
EWAISF—Electronic Warfare Avionics Integration Support Facility
EWAISP—Electronic Warfare Avionics Integration Support Program
EWIR—Electronic Warfare Integrated Reprogramming
EWIRDB—Electronic Warfare Integrated Reprogramming Database
EWO—Electronic Warfare Officer
FLTREP—Flight Report
FLR—Flagging Report
FME—Foreign Military Exploitation
FMS—Foreign Military Sales
ICWG—Interface Control Working Group

IDB—Integrated Database
IMP—Implementation Message
IOWG—Information Operations Working Group
IPC—Intermediate Processing Center (AIC, JICPAC, JAC Molesworth)
IV&V—Independent Verification and Validation
IW—Information Warfare
IWST—Information Warfare Support Team
JAC—Joint Analysis Center
JIOC—Joint Command and Control Warfare Center
JCS—Joint Chiefs of Staff
JFACC—Joint Forces Air Component Command
JFMO—Joint Frequency Management Office
JIC—Joint Intelligence Center
JSC—Joint Spectrum Center
JTF—Joint Task Force
LRU—Line Replaceable Unit
MAF—Mobility Air Forces
MAJCOM—Major Command
MD—Mission Data
MIDB—Modernized Integrated Database
MIIDS—Military Integrated Intelligence Data Systems
MIM—Maintenance Instruction Message
MISREP—Mission Report
MLV—Memory Loader Verifier
MOP—Memorandum of Policy
MSEWBBS—Multi service Electronic Warfare Bulletin Board System
MSIC—Missile and Space Intelligence Center
MTT—Mobile Training Teams
NAF—Numbered Air Force
NAIC—National Air Intelligence Center
NGB—National Guard Bureau
NGIC—National Ground Intelligence Center

NSA—National Security Agency

OB—Order of Battle

OC-ALC—Oklahoma City Air Logistics Center

OCR—Operational Change Request

OFP—Operational Flight Program

OG—Operations Group

OI—Operating Instruction

ONI—Office of Naval Intelligence

OO-ALC—Ogden Air Logistics Center

OPlan—Operational Plan

OPR—Office of Primary Responsibility

OPREP—Operational Report

OPSEC—Operations Security

OT&E—Operational Test and Evaluation

PACAF—Pacific Air Force

PLV—Program Loader Verifier

PMD—Program Management Directive

POC—Point of Contact

RC—Reprogramming Center (53 WG ((ACC)) ((53 EWG)), ECSF ((AFSOC)), and WR-ALC for some FMS supported systems)

RCS—Report Control Symbol

RDT&E—Research, Development, Test & Evaluation

RIM—Reprogramming Impact Message

ROW—Rest of World

S&TI—Scientific and Technical Intelligence

SCCSB—Software Configuration Control Subboard

SCM—Software Change Message

SEAD—Suppression of Enemy Air Defenses

SIGINT—Signals Intelligence

SIM—System Impact Message

SPO—System Program Office

SPC—Service Production Centers

STM—Stator Message

TCC—Telecommunications Centers
TCM—Technical Coordination Meeting
TCTO—Time Compliance Technical Order
TCVM—Threat Change Validation Message
TCVR—Threat Change Validation Request
ULM—Unit Loading Message
USAFE—US Air Force Europe
USG—US Government
WRM—Wartime Reserve Modes
WR-ALC—Warner Robins Air Logistics Center
WSO—Weapons Systems Officer

Terms

Automatic Digital Network (AUTODIN)—AUTODIN is a switched network of the Defense Information System which functions as a single, integrated, worldwide, high-speed, computer-controlled, general-purpose communications network.

Block Cycle—In this process the RC receives software change requests from the user, and other change requests from organizations, which are associated with the software process. The RC evaluates these requests and identifies potential solutions. When the user determines that sufficient changes have been identified to justify the expense of an update, the RC implements the software changes. Changes are scheduled based on the criticality of the requirement, with routine updates generally occurring approximately every 18 months for Operational Flight Programs (OFP) and Mission Data (MD).

BRAVE BYTE—The nickname for Army electronic warfare system changes.

Bulletin Board System (BBS)—The BBS is a means of transmitting digital data and EWIR message traffic to operational locations. Normally, data and messages are available on the BBS almost simultaneously with their transmission over AUTODIN. The BBS uses the STU-III/DCSs to transmit digital data, via commercial or Defense Switch Network (DSN) voice lines, or SIPRNET, from reprogramming centers directly to operational locations which possess STU-III/DCSs and appropriate communications software. Since the BBS is a "pull" system, units must be notified by message or telephone that new MD software has been loaded on the BBS. With the implementation of the Defense Message System, the BBS will continue to be a source for the transmission of reprogramming data and EWIR message traffic.

Data Dictionary/Directory Services—Key computer software tools that manage data and information resources. Such services provide extensive facilities for recording, storing, and processing descriptions of an organization's significant data and data processing resources, and often provide facilities to use metadata (information about data).

Defense Message System (DMS)—DMS is a flexible, secure, commercial-off-the-shelf (COTS) based system providing multi-media messaging and directory services taking advantage of the underlying Defense Information Infrastructure network and services. DMS is a new way of doing electronic

organizational messaging. DMS is eliminating the need for the Automatic DMS is a integrated suite of applications designed to run on the Defense Information System Network (DISN). DMS is NOT a network and is the system of record for "ORGANIZATIONAL" messaging and services.

Electronic Warfare (EW) Baseline for Foreign Sales—The baseline applies to both USAF inventory and non-inventory EW equipment. It establishes USAF release policy recommendations for several technology transfer issues, including EW systems, in-country reprogramming, software source code, non-inventoried systems, High Value Assets, Millimeter Wave Technology, and Electronic Attack (EA) techniques.

Electronic Warfare Integrated Reprogramming (EWIR)—The process that fully integrates operations, intelligence, communications, logistics, and other support functions to provide changes to reprogrammable electronic warfare equipment hardware and software, tactics, and equipment settings. EWIR gives the Air Force a clear and comprehensive picture of tasks, data, staffing, and the interrelationships between the agencies that reprogram EW equipment. This process forms the basis for developing Air Force procedures, organizations, facilities, and expertise to ensure responsive EW reprogramming during peacetime, wartime, and contingencies.

Electronic Warfare Integrated Reprogramming Data Base (EWIRDB)—The EWIRDB contains parametric data describing EW systems. S&TI centers, AFIWC, Army, Navy and NSA provide the data to NAIC for the purpose of merging the data and distributing it to customers. This is the primary source for mission and reprogramming data.

Emergency Reprogramming Center (ERC)—A term used by RCs when 24-hour operations (both real world and exercise) are established in response to contingencies and combat operations or as directed by MAJCOM or theater commanders. RCs will send an activation message announcing the establishment of the ERC and a deactivation message when the ERC has been deactivated to all organizations and MAJCOMs involved in the reprogramming process.

Firmware—Software that is permanently stored in a hardware device that allows reading but not writing or modifying the software. The most common device used for firmware is read-only memory.

Flagging—Comparing observed threat data to the data programmed in an electronic warfare system to determine if the threat system will be correctly identified or jammed. AFIWC maintains automated flagging models.

International Agreements—A legally binding agreement between two or more sovereign governments.

Implementation Message—Major command or Joint Forces Air Component Command, Combined Forces Air Component Command, or Air Operations Center approval to load a change that the reprogramming centers have made to electronic warfare systems and sent to the units.

Joint Coordination of EW Reprogramming (JCEWR)—The term for the joint electronic warfare systems.

Joint Universal Lessons Learned System (JULLS)—A Joint system used to track and store Lesson Learned from contingencies to exercises.

Mission Data (MD)—Elements or files a computer uses to perform signal discrimination, target a threat, or elicit jammer responses, which are selectable, adjustable, or changeable by the using command with the exception being FMS customers. MD is also called Emitter Identification Data (EID), Mission Data File (MDF), Pre-Flight Message (PFM) Code Form Message (CFM), or other related names that vary in

function according to the system using them.

NEPTUNE BYTE—The term for Navy electronic warfare system changes.

Operational Change Request (OCR)—A formal request to the appropriate major command and support command facilities that identifies the inability of an electronic warfare system to meet operational requirements. In emergencies, an OCR identifies the inability to discriminate or respond to a threat and then requests mission data or operational flight program (OFP) changes to correct the problem.

Operational Flight Program (OFP)—The executable program resident in computer-controlled electronic warfare systems that contains the algorithms that receive, identify, process, and do jamming tasks. This program does not contain any threat-specific data, and operational commands cannot change the program. The reprogramming centers send a software change message (SCM) to Air Force Materiel Command to get an OFP modified.

PACER WARE—The term for actual electronic warfare system changes issued during peacetime, contingencies, or wartime operations. PACER WARE actions can be at the routine, urgent, or emergency level as required.

PROUD BYTE—The nickname for Joint reprogramming exercises.

Rapid Reprogramming —The term used to describe the method to reprogram EW systems in a time sensitive manner.

Reprogramming Center (RC)—Its primary function is planning, designing, testing, and fielding of EW system OFP updates.

Reprogramming Centers

53EWG, Eglin AFB FL

Electronic Combat Support Flight (ECSF)

WR-ALC/LNE

WR-ALC/LNI

EW Systems

Bomber, fighter, reconnaissance and FMS systems

Special Operations, airlift, and helicopter systems

All U.S. systems

FMS systems

Security Assistance Program—A program designed to provide assistance (i.e. training, weapons, hardware) to a foreign government for furthering the US national security strategy.

SERENE BYTE—The nickname for exercising Air Force electronic warfare system changes.

Software Validation—The integration, testing, and evaluation performed at the system or subsystem level to ensure the final program satisfies the system specifications and user or supporting command requirements.

Threat Change Validation—When the responsible threat validation authority has determined a new mode is a valid operating mode of the threat system, based on available and relevant intelligence information.

Verification—Process of comparing two levels of an information system specification for proper correspondence (e.g., security policy model with top-secret specification, top-level specification with source code, or source code with object code.)

Attachment 2

EWIR SUBCOMMITTEE MEMBERSHIP MATRIX

Figure A2.1. EWIR Oversight Committee and Subcommittee Membership Matrix.

	RC SPT	COMM	OVERSIGHT
HQ USAF/XOIE	X	X	C
ILMY		X	
SCMI		X	
HQ ACC/DOZ	O	X	X
DRK	O	X	X
SCM		X	
53EWG/TA			X
68 EWS/EWP	X	C	O
36EWS	O	O	O
53 CSS/SC	X	X	O
HQ AFSOC/DOX	O	X	X
LGM			X
SCT		X	
ECSF (AFSOC)	X	X	X
HQ AMC/XPR	O		
LGB			X
DOK	O		X
SC		X	
WR-ALC/LNE	C	X	X
LNI	X	X	X
LEA			X
AIA/DO			X
AFIWC	X		X
453 EWS	X	O	X
NAIC/TAE	X		X
20 IS/EEF			X
DIA/PGI-3A			X
PO-1B			X
NSA/WM4			X

NOTES:

HQ AETC, HQ PACAF, and HQ USAFE attend subcommittee meetings as required or when HQ USAF/XOIE directs.

Key: C = Chairman; X = Member; O = Observer

Attachment 3**SAMPLE FLAGGING REPORT (FLR) FORMAT****INSTRUCTIONS:**

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: AFIWC (453 EWS)

TO: RCs, MAJCOM EWIR POCs

CC: as required (other agencies when requested)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE FLR ALQ-161 PW 01 ACC001 (U) (see **Attachment 13** for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (area) DATA PROCESSED BETWEEN (start date) AND (end date). COLLECTIONS FROM A POLYGON DEFINED BY THE FOLLOWING COORDINATES (coordinates defining the area of interest).
3. THIS REPORT CONTAINS FINDINGS THAT MAY CAUSE PROBLEMS FOR THE SUBJECT SYSTEM. IMPORTANT: PARAMETRIC INFORMATION FOUND IN SUMMARIZED SIGINT HAS INHERENT LIMITATIONS!
4. (data concerning intercept parameters and model responses)

5. (contact instructions if other than POC of message, otherwise not required)
6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 4

SAMPLE OPERATIONAL CHANGE REQUEST (OCR) FORMAT

INSTRUCTIONS:

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: Organization sending the message

TO: MAJCOM EWIR POCs

CC: as required (Appropriate RCs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE OCR ALQ-161 PW 01 ACC001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

APPLICABLE PACER WARE INFORMATION CAN BE FOUND ON THE MULTI-SERVICE ELECTRONIC WARFARE DATA DISTRIBUTION SYSTEM (MSEWDDS) AS FOLLOWS:

LIBRARY---FILE NAME---ADDED---COMMENTS

B) 161MSG, 1897RIM.RTF, 02/06/01, PACER WARE RIM ALQ-161 PW 01 AWF1

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (provide description of the specific problem).
 - A. PRIORITY: (select EMERGENCY, URGENT or ROUTINE)
 - B. SYSTEM: (complete nomenclature of the system and software version, e.g. ALR-69 SWV 0805).
3. REQUEST MACOM APPROVAL OF THE REQUESTED CHANGE AND DIRECT TO THE APPROPRIATE REPROGRAMMING CENTER TO BEING WORK (based on the priority).
4. (contact instructions if other than POC of message, otherwise not required).
5. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 5**SAMPLE SOFTWARE CANGE MESSAGE (SCM) FORMAT****INSTRUCTIONS:**

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: RC sending the message

TO: RC performing the coding of the software change

CC: as required (Appropriate MAJCOMs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE SCM ALQ-161 PW 01 ACC001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (RC providing the coding) IS AUTHORIZED TO ENCODE THE (system and SWV) MISSION DATA LISTED IN PARAGRAPH 3. THE NEW SOFTWARE WILL REPLACE (system and SWV). THIS

SOFTWARE SHOULD BE ENCODED AT (select EMERGENCY, PRIORITY or ROUTINE) PRECEDENCE. PLEASE PROVIDE THIS OFFICE WITH AN ESTIMATED COMPLETION DATE TIME GROUP.

3. (discussion of what the MD reprogramming engineer is trying to accomplish with the MD, test desired and how the resultant MD is to be released).
4. (mission data to be encoded).
5. (contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 6**SAMPLE SYSTEM IMPACT MESSAGE (SIM) FORMAT****INSTRUCTIONS:**

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: RC sending the message

TO: Wing/Groups who use the affected system

CC: as required (Appropriate MAJCOMs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE SIM ALQ-161 PW 01 ACC001 (U) (see **Attachment 13** for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (describe the threat change or problem, {for threat change provide the ELNOT/system name/function/parametric change} and its specific impact on the affected EW system)

3. (describe the indication, or lack of indication, the aircrew can expect and specific operational impact. Include recommended tactics, interim course of action and long term course of action to solve the problem).
4. ENSURE THIS INFORMATION IS MADE AVAILABLE TO ALL AIRCREWS WHO MAY BE AFFECTED.
5. (24hr contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 7

SAMPLE REPROGRAMMING IMPACT MESSAGE (RIM) FORMAT

INSTRUCTIONS:

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: RC sending the message

TO: MAJCOMs and Wing/Groups who use the affected system

CC: as required (Appropriate MAJCOMs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE RIM ALQ-161 PW 01 ACC001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (e.g. ALR-69 SWV 0806 replaces ALR-69 SWV 0805) ON THE (aircraft type). DO NOT LOAD THIS NEW SOFTWARE BVERSION INTO ANY EW SYSTEM UNLESS SPECIFICALLY AUTHORIZED TO DO SO BY YOUR IMPLEMENTATION AUTHORITY IN AN IMPLEMENTATION MESSAGE (IMP). THE OPERATIONAL IMPACT OF THE NEW SOFTWARE IS DESCRIBED IN PARAGRAPH 3. FOLLOW TCTO OR MAINTENANCE INSTRUCTION MESSAGE (MIM) INSTRUCTIONS, IF APPLICABLE. THE SOFTWARE CHANGE IS LOADED ON THE MSEWDDS (provide library and file name).
3. (describe the software change and operational impact).
4. ENSURE ALL AIRCREWS USING THE (affected system) ARE BRIEFED ON THE SOFTWARE CHANGE.

5. (24hr contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 8**SAMPLE MAINTENANCE INSTRUCTION MESSAGE (MIM) FORMAT****INSTRUCTIONS:**

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: RC sending the message

TO: MAJCOMs and Wing/Groups who use the affected system

CC: as required (Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE MIM ALQ-161 PW 01 ACC001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (specific maintenance instructions for loading the referenced software change).

3. (describe maintenance impacts, which are caused by the software change, to include additional tests that may be required.
4. IMPLEMENTATION INSTRUCTIONS: INSTALLATION OF THIS CHANGE MUST APPROVED BY YOUR IMPLEMENTATION AUTHORITY IN AN IMPLEMENTATION MESSAGE (IMP). DO NOT LOAD THE CHANGED SOFTWARE IN TO ANY EW SYSTEM UNTIL PROPER IMPLEMENTATION INSTRUCTIONS ARE RECEIVED.
5. (contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 9**SAMPLE TIME COMPLIANCE TECHNICAL ORDER MESSAGE (TCTO) FORMAT****INSTRUCTIONS:**

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: RC sending the message

TO: MAJCOMs and Wing/Groups who use the affected system

CC: as required (Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE TCTO ALQ-161 PW 01 ACC001 (U) (see **Attachment 13** for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (describe the difference the Block Cycle or OFP change implemented over the superseded software).
3. (describe any changes to system Handbooks and or Mission Guides).

4. (describe any changes to Mission Data).
5. IMPLEMENTATION INSTRUCTIONS: YOUR IMPLEMENTATION AUTHORITY HAS APPROVED INSTALLATION OF THIS CHANGE. AT RECEIPT OF REFERENCED TCTO, INSTALL THE SOFTWARE CHANGE AFTER PROPER COORDINATION WITH THE WING/ GROUP EW POC IAW AFI 10-703.
6. (contact instructions if other than POC of message, otherwise not required).
7. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 10

SAMPLE IMPLEMENTATION MESSAGE (IMP) FORMAT

INSTRUCTIONS:

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: MAJCOM or JFACC/CFACC/AOC

TO: Wing/Groups in area of responsibility who use the affected system

CC: as required (Appropriate RCs and other agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE IMP ALQ-161 PW 01 ACC001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

APPLICABLE PACER WARE INFORMATION CAN BE FOUND ON THE MULTI-SERVICE ELECTRONIC WARFARE DATA DISTRIBUTION SYSTEM (MSEWDDS) AS FOLLOWS:

LIBRARY----FILE NAME----ADDED----COMMENTS

B) 161MSG, 1897RIM.RTF, 02/06/01, PACER WARE RIM ALQ-161 PW 01 AWF1

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. THIS MESSAGE IS HQ ACC/DO AUTHORIZATION TO INSTALL REFERENCED SOFTWARE CHANGE TO B-1 AIRCRAFT SPECIFIED IN THE RIM. TRAINING/TEST UNITS WILL UPLOAD THE SOFTWARE CHANGE ON A NON-INTERFERENCE BASIS WITH PROGRAMMED TRAINING AND TESTING.
3. ENSURE THAT THIS MESSAGE IS MADE AVAILABLE TO YOUR DEPLOYED UNITS, IF APPLICABLE.
 - A. DEPLOYED UNITS ASSIGNED TO OPERATION NORTHERN WATCH (ONW) MUST WAIT FOR IMPLEMENTATION FROM USAFE/DOTW.
4. THIS MESSAGE CAN BE FOUND ON THE MSEWDDS EITHER BY SECURE STU-III MODEM OR THROUGH SIPRNET AT [HTTP://WWW.WG53.EGLIN.AF.SMIL.MIL](http://www.wg53.eglin.af.mil) OR ([HTTP://207.84.75.101](http://207.84.75.101)). MSEWDDS ASSISTANCE CAN BE OBTAINED BY CALLING DSN 872-2166. THE REFERENCES ABOVE INDICATE THE APPROPRIATE BBS LIBRARY AND FILE NAME FOR SUBJECT MESSAGES.
5. IMPORTANT: PER REFERENCE A, UNITS ARE REQUIRED TO PROVIDE A UNIT LOADING MESSAGE (ULM) NLT 1 MAR 01 OR AS SOON AS LOADING IS COMPLETE. THIS CAN BE DONE BY REPLYING TO THE DMS IMP MESSAGE OR E-MAIL <mailto:ACCDOZO@LANGLEY.AF.MIL>. COURTESY COPY (CC) THE 53WG PW ACCOUNT FOR DMS MESSAGES OR INFO <mailto:53WGERCPW@EGLIN.AF.MIL> IF E-MAIL.
 - A. DEPLOYED UNITS ASSIGNED TO ONW ARE REQUIRED TO PROVIDE A ULM TO USAFE AS SOON AS LOADING IS COMPLETE.
6. UNITS EXPERIENCING DIFFICULTIES SHOULD CONTACT THE POC TECHNICAL SUPPORT NUMBER(S) FOUND WITHIN THE RIM.
7. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 11**SAMPLE UNIT LOADING MESSAGE (ULM) FORMAT****INSTRUCTIONS:**

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: Wing/Group sending the message

TO: MAJCOMs or JFACC/CFACC/AOC IMP Authority

CC: as required (RCs and Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE ULM ALQ-161 PW 01 ACC001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.

2. THE (wing/group i.e. 1FW) HAS COMPLETED LOADING REFERENCE SOFTWARE CHANGE. LOADING WAS COMPLETED ON (DTG in ZULU i.e. 12 2345 DEC 01).
3. (any pertinent information concerning delays in loading, problems in lading etc. otherwise not require).
4. CONTACT INSTRUCTIONS:
 - A. WING/GROUP EW POC: (name, rank, phone number and unclassified e-mail address).
 - B. WING/GROUP AVIONICS/POD SHOP POC: (name, rank, phone number and unclassified e-mail address).
5. THIS IS AN AIR FORCE PACER WARE MESSAGE.

CLASSIFIED BY: (use applicable source)

DECL: (provide appropriate declassification information)

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 12

SAMPLE STATUS MESSAGE (STM) FORMAT

INSTRUCTIONS:

1. Follow Defense Message System (DMS) standard formatting rules.
2. For DMS address listings, check the DUA Browser.
3. Message identification number (e.g. PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001) **must** be in the subject line.
4. Subject line **must** contain the classification (unclassified/confidential/secret) of the message body followed by DMS Precedence – “ROUTINE or IMMEDIATE” at the start of the subject line e.g. (C) DMS ROUTINE, PACER WARE OCR ALR-69 SWV 0805 PW 00 AWF001 (U) **Subject line should always be unclassified.**
5. For exercise messages use EXERCISE in place of PACER WARE. **Do not use both.**
6. Message body will **always** have classification markings starting at the top and bottom.

EXAMPLE:

FROM: RC sending the message

TO: MAJCOMs or JFACC/CFACC/AOC IMP Authority

CC: as required (Appropriate Agencies)

SUBJECT: (classification of message body) DMS ROUTINE, PACER WARE STM 53 EWG/ERC PW 01 AWF001 (U) (see [Attachment 13](#) for message designations standards)

MESSAGE BODY:

(UNCLASSIFIED / CONFIDENTIAL / SECRET)

(reference all pertinent information)

REF/A/DOC/HQ ACC DOZ/(date)

REF/B/MSG/(originators office)/(date)

REF A IS AFI 10-703, PROVIDES POLICY AND PROCEDURES FOR ELECTRONIC WARFARE INTEGRATED REPROGRAMMING (EWIR).

REF B IS (message e.g. PACER WARE (PW) REPROGRAMMING IMPACT MESSAGE (RIM) ALQ-161)

POC/(rank and name of author, office symbol, telephone number and e-mail address)

1. THIS IS AN AIR FORCE PACER WARE MESSAGE.
2. (provide the time frame covered by this STM).
3. STATUS OF: (the following paragraphs will be provided for each system the reprogramming center is responsible for).
 - C. SYSTEM NAME:
 - D. DTG OF SCM's OR TASKING RECEIVED:
 - E. TESTING COMPLETE: (estimated or actual time).
 - F. ENGINEERING COMPLETE: (estimated or actual time).
 - G. KIT PROOF: (estimated or actual time).
 - H. DISTRIBUTE: (estimated or actual time).
 - I. MESSAGE SERIAL NUMBER: (i.e. MIM ALR-69 SWV 0806 PW 00 AWF001).
 - J. SYSTEM POC's: (engineers and or equipment specialists).

- K. COMMENTS: (list any known problems or any field confirmations received or distributed reprogramming data packages).
4. STATUS OF: (paragraph 3 is repeated again for each system).
5. (contact instructions if other than POC of message, otherwise not required).
6. THIS IS AN AIR FORCE PACER WARE MESSAGE.
- CLASSIFIED BY: (use applicable source)
- DECL: (provide appropriate declassification information)
- (UNCLASSIFIED / CONFIDENTIAL / SECRET)

Attachment 13

EWIR MESSAGE DESIGNATION STANDARDS FOR THE SUBJECT LINE

EXAMPLE: PACER WARE OCR ALR-69 SWV 0805 PW 95 AWF001 (U)

(1) (2) (3) (4) (5, 6) (7, 8) (9)

(1) Type of Change:

PACER WARE: An **Actual** reprogramming change

EXERCISE: An **Exercise** reprogramming change

(2) Type of Message:

TCVR: Threat Change Validation Request

TVM: Threat Change Validation Message

FLR: Flagging Reports

OCR: Operational Change Request

SIM: System Impact Message

RIM: Reprogramming Impact Message

MIM: Maintenance Instruction Message

TC TO: Time Compliance Technical Order

IMP: Implementation Message

ULM: Unit Loading Message

STM: Status Message

RTM: Request for Transmission Message (Foreign Military Sales Only)

RRM: Request for Release Message (Foreign Military Sales Only)

RAM: Release Authorization Message (Foreign Military Sales Only)

(3) Equipment Designation:

Do not use slashes (/) (for example, ALR-69, ALR-56C, and so forth).

Include three-letter command or nation identifier for multi-command and multinational systems (for example, ALR-69 (KOR), ALQ-172 (V) 2 (SOC)).

(4) Software Version Code (SWV):

Use the three-letter designation "SWV" followed by the version number of the software this particular message addresses.

(5) Situation Code:

Two letter designation for:

Actual changes (PW - PACER WARE).

MAJCOM exercises (Q1 through Q4) NOTE: Quarters are based upon calendar year quarters, i.e., Jan - Mar = Q1, etc.

Air Force exercise (EX - EXERCISE).

Tests (T1, T2, T3...).

Other specified two-letter code.

(6) Calendar-Year Designation:

Two number designation for the current calendar year (for example, 95 for 1995, 96 for 1996, and so forth).

(7) Originator's Designation:

ACC	Air Combat Command
AET	Air Education and Training Command
IWC	AFIWC
USA	HQ USAF
AWI	53 EWG (FMS Programs)
AWF	53 EWG (USAF Programs)
PCF	PACAF
SOF	ECSF (AFSOC)
SOC	AFSOC
AFE	USAFE
WLA	Wright Labs
RLI	WR-ALC/LNI
RLN	Warner Robins Air Logistics Center
AMC	Air Mobility Command
ANG	Air National Guard
AFR	Air Force Reserve Command

Unit Codes: Codes for individual units are based on their distinctive unit aircraft identification markings (tail codes). The last letter will be the wing or squadron identifier (Z or A through Y). If the wing consolidates the reports for its subordinate units, use the letter "Z". If the individual squadrons will be submitting the reports, use A through Y, starting with the lowest numbered squadron using the letter "A", the next lowest numbered squadron using the letter "B", etc. Provisional units and units without tail codes generate an originator identifier with their MAJCOM.

(8) Three-Digit Sequence Number Designation:

Number each message sequentially by system and message type for each **calendar** year (for example, 001 for the first ALR-69 OCR of a certain year, 002 for the next ALR-69 OCR for that same year, and so on).

NOTE: The first RIM for an ALQ-184 reprogramming action will also be 001. Do not attempt to follow other originators' numbering sequences.

(9) Subject Line Classification:

Always keep the subject line of PACER WARE or Serene Byte messages UNCLASSIFIED.