BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 91-105

10 DECEMBER 1993

Safety

CRITICAL COMPONENTS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

OPR: HQ AFSA/SENA (Maj Glenn H. Carroll)

Certified by: HQ USAF/SE
(Brig Gen James L. Cole, Jr.)

Supersedes AFR 122-17, 4 December 1989

Pages: 4
Distribution: F

This instruction implements AFPD 91-1, *Nuclear Weapons and Systems Surety*. It outlines requirements for transporting, storing, handling, and using critical components and explains the process for certifying and decertifying critical components. It applies to all organizations that have a mission involving operations, maintenance, security, or logistics movement of critical components and certified software. It does not apply to Air Force Reserve and Air National Guard units and members. Send major command (MAJCOM) supplements to HQ AFSA/SENA, 9700 Avenue G, Kirtland AFB NM 87117-5671) for coordination and to HQ USAF/SE, 1400 Air Force Pentagon, Washington DC 20330-1400, for approval before publication.

SUMMARY OF REVISIONS

This is the initial publication of AFI 91-105, substantially revising AFR 122-17, 4 December 1989. It cross-references the terms and definitions in AFI 91-101; moves the list of critical components, tamper detection indicators (TDI), and certified software to a technical order; clarifies use of labels or tags to identify critical components that need Two-Person Concept control; allows transport of critical components by the Defense Courier Service; and incorporates provisions for using TDIs on critical components for storage.

Section A—Terms, Goals, and Responsibilities

1. Terms and Definitions. For definitions of terms used in this instruction, see AFI 91-101, *Air Force Nuclear Weapons Surety Program* (formerly AFR 122-1).

2. Air Force Goal. Bypassing, activating, or tampering with critical components could lead to activation of a critical function or could otherwise degrade nuclear surety. To prevent unauthorized activation of critical functions, the Air Force develops positive measures to protect against inherent risks and threats, and to ensure components are compatible with the assembled nuclear weapon system.

3. Responsibilities:

3.1. Air Force Chief of Safety (HQ USAF/SE). HQ USAF/SE establishes requirements to designate, certify, and manage critical components. Acting for HQ USAF/SE, the Commander of the Air Force Safety Agency, manages the process and directs HQ AFSA/SEN to:

- Designate appropriate hardware, software, media, or code components as critical components.
- Designate split-handling or split-knowledge procedures for critical components.
- Approve vaults and containers for storage of critical components.
- Approve use of Tamper Detection Indicators (TDI) and certify their design, as specified in AFI 91-103, *Air Force Nuclear Safety Certification Program* (formerly AFR 122-3), for use in protecting the certification status of critical components.
- Maintain lists of design-certified hardware and software, critical components, and TDIs in Technical Order (TO) 00-110N-16, *Equipment Authorized for Use With Nuclear Weapons.*

3.2. Nuclear Weapon System Safety Group (NWSSG). The NWSSG recommends components for critical component status. The NWSSG recommendations are approved or disapproved at Air Staff level and must indicate:

3.2.1. At what point in its life cycle a component will be operationally certified.

3.2.2. Whether split-handling or split-knowledge control procedures are recommended and at what point in the component's life cycle to apply the procedures.

3.3. Major Commands. Major commands do the following:

- Recommend items for critical component status to HQ AFSA/SEN.
- Recommend design decertification of critical components to HQ AFSA/SEN.
- Implement split-handling and split-knowledge control procedures.
- Use only design-certified hardware and software in an operational nuclear weapon system.
- Operationally certify critical components, as required by approved procedures, before using them in operational nuclear weapon systems.
- Decertify critical components according to AFI 91-103.
- Ensure critical components are properly marked.
- Control certified critical components according to **Section C** of this instruction.

Section B—Designating and Marking Critical Components

4. Designating Critical Components. Critical components must receive nuclear safety design certification following the guidelines in AFI 91-103.

4.1. All items designated as critical components must pass operational certification procedures before use.

4.2. The National Security Agency (NSA) may request critical component designation for NSA-produced software and hardware used with a nuclear weapon or nuclear weapon system. The NSA software and hardware items receive design certification equal to that provided by the Air Force and do not need additional Air Force design certification.

5. Marking Critical Components. A command using critical components identifies those that need control under the Two-Person Concept with labels or tags. Follow these guidelines:

5.1. Affix the label (or tag, if the component is too small for a label) to the outside of the critical component or the component's shipping container.

5.2. Remove or cover the label or tag when the component is not certified for operational use.

5.3. Do not use external markings to identify areas, facilities, aircraft, or equipment as containing critical components.

Section C—Controlling Critical Components

6. Two-Person Concept. The Two-Person Concept protects a part of each critical component's life cycle. This minimizes the possibility that an unauthorized or inadvertent act could degrade the nuclear surety of a nuclear weapon or nuclear weapon system. Two-Person Concept control for a critical component may begin at the time of production and continue until the critical component's destruction, or may occur during any part of that time. Complete the following tasks:

6.1. Handle and control the component following the guidelines for operationally certified critical components in AFI 91-104, *Nuclear Surety Tamper Control and Detection Programs* (formerly AFR 122-4). Remarks in TO 00-110N-16 may provide additional guidelines for particular components.

6.2. Keep a code component or device under Two-Person Concept control, or store it according to the methods described in paragraphs **9.1.1.** to 9.1.2 when an operational code that you can't overwrite passes through it. Also apply Two-Person Concept control if the code component or device has no operational decertification procedure. Continue Two-Person Concept control until all codes that passed through it are superseded.

7. Operational Use of Critical Components. Protect certified critical components in operational use by keeping them under Two-Person Concept control or in a storage facility as specified in paragraphs **9.1.1.** to 9.1.2.

8. Shipping Requirements. If using a Two-Person Concept team or approved TDIs to protect the certification status, you may use the Department of Defense Courier Service to transport operationally certified critical components.

9. Storage Requirements. These storage requirements apply to certified critical components. Decertified critical components only require the special storage needed to meet security classification requirements.

9.1. Use one of the following methods to store certified critical components that are not under Two-Person Concept control:

9.1.1. Method 1. Store components in an approved reinforced concrete vault. Use an intrusion detection system reporting to a remote, continuously staffed location.

9.1.2. Method 2. Store components in an approved storage container. Use a volumetric motion detector and adoor detector. Both detectors must report independently to a remote, continuously staffed location.

9.1.3. Method 3. Protect components with TDIs approved under AFI 91-104.

9.2. Apply the following for methods 1 and 2:

9.2.1. Store the component in a no-lone zone.

9.2.2. Secure every entrance to the no-lone zone with two General Services Administration medium-security locks and ensure no individual can open both locks.

9.2.3. Incorporate a line supervision scheme in the alarm reporting circuits that detects tampering and reports it to the remote, continuously staffed location as an alarm.

9.2.4. Keep at least one person focused on security functions at the alarm monitor location.

9.3. Unless they are protected by method 3, keep certified critical components that are in temporary storage (such as uncoded Minuteman missile guidance sets remaining overnight at launch control facilities) in a no-lone zone. Protect the components as their classification warrants.

JAMES L. COLE, JR., Brig Gen, USAF
Chief of Safety