BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 91-103

16 SEPTEMBER 2005

Safety

AIR FORCE NUCLEAR SAFETY DESIGN CERTIFICATION PROGRAM

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFSC/SEWE

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

Supersedes AFI 91-103, 26 June 2001

Pages: 23

This instruction implements AFPD 91-1, *Nuclear Weapons and Systems Surety*. It defines the process for obtaining nuclear safety design certification of hardware, software, procedures and facilities used with nuclear weapon systems. It applies to organizations that design, develop, modify, evaluate, or operate nuclear weapon systems. It does not apply to the Air Force Reserve and Air National Guard. Send proposed supplements to this instruction to HQ AFSC/SEW, 9700 G Avenue, Kirtland AFB NM 87117-5670, for coordination and approval before publication. **Attachment 1** lists abbreviations and acronyms used in this instruction. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with AFPD 37-1, *Information Management* and AFMAN 37-123, *Management of Records,* and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at **https://webrims.amc.af.mil**.

SUMMARY OF CHANGES

This document is substantially revised and must be completely reviewed. It requires nuclear safety design certification for facilities used to support, maintain, handle or store nuclear weapons and expands on the certification requirements of vehicles. It establishes nuclear safety design certification process requirements outlined in AFI 63-125, *Nuclear Certification Program*. In addition, organization names were updated to reflect changes since the last publication of this instruction.

Section A—Scope and Responsibilities

1. Definitions. See AFI 91-101, *Air Force Nuclear Weapons Surety Program*.

2. Program Goal. The Air Force Nuclear Safety Design Certification Program evaluates hardware, software, procedures, and facilities against specific nuclear safety criteria before use with nuclear weapons. The program's goal is to prevent nuclear weapon accidents and incidents.

3. Responsibilities.

3.1. **Chief of Safety (HQ USAF/SE).** HQ USAF/SE oversees the Air Force Nuclear Safety Design Certification Program that is an integral part of the overall Air Force Nuclear Certification Process.

3.2. **HQ AFSC/SEW** manages the nuclear safety design certification program for HQ USAF/SE. In this role, HQ AFSC/SEW will:

3.2.1. Publish design and evaluation criteria according to AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon System*s.

3.2.2. Review and coordinate on nuclear certification impact statements (NCIS) that affect nuclear safety design certification.

3.2.3. Approve the Nuclear Safety Certification annex to the Certification Requirements Plan (CRP) to ensure nuclear safety design certification requirements are adequately addressed.

3.2.4. Approve new or revised test and weapon maintenance procedures for nuclear weapons performed in Air Force facilities.

3.2.5. Review Nuclear Surety Evaluations (NSE) for compliance with all nuclear safety design certification requirements.

3.2.6. Provide nuclear safety design certification of hardware, software, procedures, and facilities to be used with nuclear weapons.

3.2.7. Issue a Nuclear Safety Certification Letter to Air Armament Center/Certification Management Division (AAC/NWC) upon completion of all nuclear safety design certification actions identified in the CRP.

3.2.8. Designate and certify critical components according to AFI 91-105, *Critical Component*s.

3.2.9. Certify Tamper Detection Indicators (TDI).

3.2.10. Identify nuclear safety designed certified hardware and software items, and restrictions on usage, to AAC/NWC for listing in the master nuclear certification list (MNCL).

3.2.11. Approve ICBM operational certification (OPCERT) and decertification (DECERT) procedures.

3.2.12. Rescind nuclear safety design certification of hardware, software, and facilities.

3.2.13. Review Nuclear Explosive-Like Assembly (NELA) maintenance.

3.3. **MAJCOM Responsibilities.** The MAJCOM operating the system will:

3.3.1. Establish a nuclear safety design certification program.

3.3.2. Designate a person to manage the nuclear certification program IAW AFI 63-125, *Nuclear Certification Program*.

3.3.3. Provide guidance to units on the nuclear safety design certification program (send copy to HQ AFSC/SEW for review).

3.3.4. Request a nuclear certification impact statement (NCIS) IAW AFI 63-125, *Nuclear Certification Program*, be prepared by the organization with program management responsibility, for non-certified equipment for which use with nuclear weapons is desired.

3.3.5. Identify new uses for certified TDIs and request approval from HQ AFSC/SEW.

3.3.6. Ensure ICBM critical components are operationally certified (OPCERT) before use.

3.3.7. Ensure nuclear units report deficiencies on certified items according to procedures in AFMAN 91-221, *Weapons Safety Investigations and Report*s.

3.3.8. Serve as the Single Manager for the certification and configuration control of facilities (as defined in paragraph **4.1.9.**) to include lifting and suspension systems.

3.3.9. When serving as the Single Manager for facility certification:

3.3.9.1. Prepares NCIS in accordance with AFI 63-125, *Nuclear Certification Program*, to support the nuclear safety design certification process of **Section C**, paragraph **7.2.**

3.3.9.2. Develop the Nuclear Safety Certification annex to the Certification Requirements Plan (CRP) for each facility to be nuclear safety design certified IAW AFI 63-125, *Nuclear Certification Program*.

3.3.9.3. Ensure processes, policy, and guidance are in place to maintain configuration control of nuclear safety design certified facilities.

3.3.9.4. Conduct NSE of the facilities used with a nuclear weapon system.

3.3.9.5. Review deficiencies (materiel deficiency reports, service bulletins, and nuclear safety deficiency reports) for possible impact on facility certification status and implement required corrective action.

3.3.9.6. Evaluate nuclear surety compliance for facilities used with a nuclear weapon system.

3.4. **Air Force Materiel Command (AFMC).** In addition to the responsibilities outlined in paragraph **3.3.**, AFMC will:

3.4.1. Ensure processes, policy, and guidance are in place for AFPEO programs, SPOs, single managers, etc., to maintain configuration control of nuclear safety design certified hardware, software, and procedures.

3.4.2. Air Armament Center Nuclear Weapons Directorate (AAC/NW) will:

3.4.2.1. Provide independent technical support (analyses, assessments, evaluations, reviews, etc.) to HQ AFSC/SEW.

3.4.2.2. Maintain archives of all pertinent documentation related to nuclear certification.

3.4.2.3. Ensure AFSC/SEW and AFNWCA are notified about nuclear weapon maintenance or test procedures not defined as a weapon ALT or MOD (see paragraph **12.**), that will be accomplished in Air Force facilities.

3.4.3. **Single Manager(s)** :

3.4.3.1. Has ultimate program management responsibilities for execution of the nuclear safety design certification program.

3.4.3.1.1. Designates a nuclear certification manager (NCM) in accordance with AFI 63-125, *Nuclear Certification Program*, to serve as the Single Manager's primary representative within the program office for day-to-day management and execution of the nuclear safety certification program.

3.4.3.1.2. Ensures NCM receives nuclear certification manager training as required by AFI 63-125, *Nuclear Certification Program*.

3.4.3.2. Prepares NCIS in accordance with AFI 63-125, *Nuclear Certification Program*, to support the nuclear safety design certification process of **Section C**, paragraph **7.2.**

3.4.3.3. Develops the Nuclear Safety Certification annex to the CRP for each weapon system or subsystem to be nuclear safety design certified IAW AFI 63-125, *Nuclear Certification Program*.

3.4.3.4. Performs unauthorized launch (UL) studies according to AFI 91-106, *Unauthorized Launch and Launch Action Studies.*

3.4.3.5. Supports the TDI development and evaluation process.

3.4.3.6. Conducts NSE of the hardware, software and procedures, used with a nuclear weapon or weapon system.

3.4.3.7. Evaluates support equipment provided by other DOD agencies for use with Air Force procedures.

3.4.3.8. Evaluates Air Force use of Department of Energy (DOE)-certified equipment with nuclear weapons to determine whether operating environments are identical and if any differences impact nuclear surety.

3.4.3.9. Ensures all certified items are marked (when possible) with labels (e.g. data plates) to enable positive identification.

3.4.3.10. Reviews deficiencies (materiel deficiency reports, service bulletins, and nuclear safety deficiency reports) for possible impact on nuclear surety or certification status and implements required corrective action.

3.4.3.11. Ensures all procedures involving nuclear safety processes are marked with the "Nuclear Surety Procedures" (NSP) symbol to enable positive identification. Special emphasis must be applied to the NSP to protect against degrading or rendering ineffective the critical nuclear safety features of the weapon system.

3.4.3.12. Develops ICBM OPCERT and DECERT procedures.

3.4.3.13. Monitors nuclear surety for hardware, software and procedures used with a nuclear weapon or nuclear weapon system.

3.5. **Assistant Secretary of the Air Force (Acquisition), (SAF/AQ).** SAF/AQ will ensure a nuclear certification program is established and that Air Force Program Executive Officers (AFPEOs), Desig-

nated Acquisition Commanders (DACs), and Single Managers for nuclear weapon systems or other items requiring nuclear safety certification comply with the requirements of this AFI.

3.6. **Air Force Nuclear Weapons and Counterproliferation Agency (AFNWCA).** AFNWCA will ensure AFSC/SEW is notified about nuclear weapon alterations (ALTs) and modifications (MODs), as defined in paragraph **12.**, that will be accomplished in Air Force facilities.

Section B—Nuclear Safety Design Certification Criteria

4. Items That Require Nuclear Safety Design Certification.

4.1. Hardware and Software:

4.1.1. Combat and noncombat delivery vehicles.

4.1.2. Operational and support equipment used to move, support, store, handle, load and unload, or mate and demate nuclear weapons.

4.1.3. All hardware and software components that directly interface (electrically or physically) with a nuclear weapon, critical component, certified software, or are identified in a current launch activation path.

4.1.4. Items that could degrade the nuclear command, control, and status reporting capability.

4.1.5. All new and currently certified critical components and software.

4.1.6. All hardware or software used to directly control critical functions as defined in AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems.*

4.1.7. TDIs used in an operational system, as well as TDIs used in a nonoperational environment for storage and transportation.

4.1.8. Operational and maintenance hardware and software used to command and control critical functions and perform status reporting.

4.1.9. Nuclear Weapons Maintenance, Handling and Storage Facilities. Nuclear safety design certification of facilities will be based on the design and evaluation of critical facility systems in accordance with AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems*.

4.1.10. Modifications to nonspecialized equipment that could impact the item's primary structure, electrical and hydraulic power systems, load-bearing capacity, steering and braking capability, or positive control features as well as any changes resulting in noncompliance with specific AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems,* design criteria.

4.1.11. Test equipment that:

4.1.11.1. Verifies the proper operation of the critical function circuits of a combat delivery vehicle or directly interfaces with nuclear weapons or operationally certified critical components.

4.1.11.2. Is used to operationally certify, decertify, or verify proper operation of applicable items identified in this paragraph unless other means of verification are used.

4.1.11.3. Is used in special test or maintenance programs to identify system anomalies or failures.

4.2. Procedures. Nuclear weapon system technical order procedures involving ICBM OPCERT or DECERT. Other nuclear weapon or nuclear weapon system technical order procedures are certified IAW AFI 63-125, *Nuclear Certification Program*.

4.3. Other. When items do not clearly fall into any of the categories identified, HQ AFSC/SEW determines if nuclear safety design certification is required.

4.4. Non-Specialized Commercial Off-the-Shelf (COTS) Equipment and Other Agency Items. The following are considered to be nuclear safety design certified, and therefore do not require separate Air Force nuclear safety design certification actions provided the item is in its original unmodified condition and is used in its intended operating environment IAW approved technical data. Modifications or deviations from original manufacturer's specifications must be approved by AFSC/SEW.

4.4.1. Tiedown chains and cables, straps, and adjusters used for restraint during transportation.

4.4.2. Support equipment and procedures for nuclear logistics movements that other DOD agencies have certified for nuclear weapons handling.

4.4.3. DOE Test, Handling, and Support Equipment provided by DOE to the Air Force for use with nuclear weapons or nuclear weapons systems, provided the equipment is used for the specific purpose intended as outlined in approved JNWPS publications, special procedures, or authorized Unsatisfactory Reports (UR) responses.

4.4.4. Commercial Vehicles.

4.4.4.1. CONUS.

4.4.4.1.1. Commercial truck-tractors, which meet the following requirements, are nuclear safety design certified. These vehicles are authorized for towing certified semi-trailers only.

4.4.4.1.2. 1979 model year or newer.

4.4.4.1.3. Gross vehicle weight greater than 25,000 pounds.

4.4.4.1.4. Manufactured in the United States or Canada.

4.4.4.1.5. Manufactured by one of the following companies: Navistar (including International Harvester Co.), Chrysler (or Daimler Chrysler) Motor Corp. (including Dodge), General Motors Corp. (including Chevrolet), Ford Motor Co, White Motor Corp, Mack Truck Co, Sterling, Freightliner.

4.4.4.2. OCONUS.

4.4.4.2.1. Commercial truck-tractors, which meet the following requirements, are nuclear safety design certified and are authorized for towing nuclear certified semi-trailers.

4.4.4.2.2. 1998 model year or newer.

4.4.4.2.3. Tractor is a type "N1 or N2" (per EC Directive 70/156/EEC Annex II and 97/27/EC).

4.4.4.2.4. Meet all applicable EUROPEAN COMMUNITY (EC)-standards

4.4.4.2.5. Must be compatible with the nuclear certified semi-trailers (i.e. braking system, electrical system, mechanical mate/de-mate, etc.).

4.4.4.2.6. Incorporate a transmission/starter interlock system.

4.4.5. Tow Vehicles:

4.4.5.1. Original equipment pintle assemblies are nuclear safety design certified. Replacements are considered certified if procured and installed per appropriate tech orders.

4.4.5.2. Vehicles modified in accordance with TO 36A-I-1341 or 36A-I-1331 for alternative fuels are considered nuclear safety design certified.

4.4.6. Semi-trailers:

4.4.6.1. Non-specialized semi-trailers are considered nuclear safety design certified when they are in original unmodified condition and meet applicable industry standards.

4.4.6.2. The addition of a certified rollerized conveyor or other like item to an uncertified trailer does not certify that trailer, even if the stock number changes to a certified number. To have a certified unit, both the trailer and the modification kit are required to be separately certified.

5. Items That Do Not Require Nuclear Safety Design Certification.

5.1. Common items:

5.1.1. General purpose handtools such as pliers, wrenches, and screwdrivers.

5.1.2. Depot and intermediate-level test equipment if the critical circuits of the tested items are verified at the organizational level before use with nuclear weapons.

5.1.3. Common, multipurpose, and nonspecialized test equipment such as multimeters, decade resistance boxes, and impedance bridges unless the equipment directly interfaces with nuclear weapons or is part of an end item that is nuclear safety design certified.

5.1.4. Delivery, Loading, Mating, Maintenance, and Explosive Ordnance Disposal (EOD) Training Equipment. All Air Force equipment designed and used for proficiency training such as full-scale and miniature practice delivery bombs and bomb dispensers, practice loading bombs and warheads, training re-entry vehicles and payload sections, EOD disassembly/reassembly training equipment, etc., do not require nuclear safety design certification.

5.1.5. Aircraft Mission Planning Software. Aircraft mission planning system software is not nuclear safety design certified. However, aircraft mission planning software that transfers operational flight program (OFP) software and cruise missile targeting data must ensure the integrity of data during this process is maintained. Mission planning systems must be designed and implemented such that:

5.1.5.1. During the transfer from one media source to another, the OFP software containing nuclear critical functions and the mission data containing nuclear targeting data, are not altered.

5.1.5.2. Integrity of the data is maintained when loaded on the aircraft.

5.1.5.3. Procedures are formulated and implemented that satisfy these nuclear surety requirements and ensure future software revisions will not alter those modules that perform the verification tasks.

5.1.5.4. New mission planning systems (e.g., Joint Mission Planning System [JMPS]) must be documented in an NSE and submitted to AFSC/SEW for approval with a copy to AAC/NWC to document the manipulation, processing and protection of flight software and nuclear targeting data.

6. Additional Requirements. The following requirements apply to critical components, TDIs, special test and maintenance programs, and host nation-operated weapon systems and procedures:

6.1. Critical components also require OPCERT before use in operational systems to verify the component is functioning as design certified and to mitigate all credible UL threats and scenarios. (Refer to AFI 91-105, *Critical Components,* and AFI 91-106, *Unauthorized Launch and Launch Action Studies*.) Certain critical components also require specific procedures for DECERT.

6.2. TDIs may be used to protect the certification status of critical components if sufficient justification exists for their use. However, TDIs may not be used to substitute for Two-Person Concept control of codes, coded devices, or critical components exposed to operational codes that cannot be decertified. TDIs used in an operational system are identified in the safety rules for the affected nuclear weapon system according to AFI 91-104, *Nuclear Surety Tamper Control and Detection Program*s.

6.3. Special test or maintenance programs conducted in operational facilities that are not covered by certified procedures must be approved by HQ AFSC/SEW.

6.4. When used with nuclear weapons in Air Force custody, host nation-operated nuclear weapon systems and procedures must satisfy the same nuclear safety criteria required for Air Force systems and procedures.

Section C—Nuclear Safety Design Certification Process

7. Nuclear Safety Design Certification Process for New or Modified Weapon System Hardware and Software. Use the following paragraphs in conjunction with AFI 63-125, *Nuclear Certification Program,* to determine the steps and timelines for the nuclear safety design certification process.

7.1. The operational MAJCOM or Single Manager identifies items that may require nuclear safety design certification according to paragraph **4.**

7.1.1. The single manager (for facilities, the single manager refers to the lead or using command) must maintain configuration control of identified hardware, software, and facilities to be nuclear safety design certified throughout their life-cycle.

7.2. For new weapon systems or weapon system modifications, the Single Manager or MAJCOM prepares an NCIS in accordance with AFI 63-125, *Nuclear Certification Program*.

7.2.1. The NCIS must address those items that require certification and recommend a certification approach for verifying compliance with AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems,* AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems*, and AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems Software***.**

7.3. The NCIS is evaluated and basic nuclear safety design certification requirements are levied in the Basic Certification Requirements Plan submitted by AAC/NWC in response to the NCIS (reference AFI 63-125, *Nuclear Certification Program*).

7.4. As the development or modification effort nears completion (determined by the required operational capability or certification need date), the Single Manager or MAJCOM prepares a NSE according to **Attachment 2**, paragraph **A2.2.** and a nuclear safety design certification recommendation as specified in **Attachment 4**. Submit the evaluation and certification recommendation to HQ AFSC/SEW. Provide a copy to AAC/NWC. If required, HQ AFSC/SEW will task AAC/NW to perform an independent nuclear surety review. ***NOTE:*** For new (and some modified) weapon systems, a Nuclear Safety Analysis Report (NSAR) typically serves as the NSE.

7.4.1. If a DOD 3150.2-M*, DOD Nuclear Weapon System Safety Program Manual*, safety study is required, submit the evaluation to HQ AFSC/SEW 120 calendar days prior to the study IAW AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules*.

7.4.2. If a safety study is not required, submit the evaluation 60 calendar days prior to the required operational capability or certification need date.

7.5. When tasked by HQ AFSC/SEW, AAC/NW reviews the design, evaluation, and certification recommendation according to **Attachment 2**, paragraph **A2.3.** and provides this assessment to HQ AFSC/SEW.

7.5.1. When a safety study is required, this assessment is submitted as required by AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules,* in the form of a Technical Nuclear Safety Analysis (TNSA).

7.5.2. If a safety study is not required, AAC/NW must submit the assessment 20 calendar days prior to the required operational capability or certification need date.

7.6. HQ AFSC/SEW will provide a Nuclear Safety Certification letter to AAC/NWC in accordance with AFI 63-125, *Nuclear Certification Program* (with a copy to Single Manager). ***NOTE:*** Restrictions on the use of items in a nuclear role may be imposed to compensate for design deficiencies or significant operational hazards.

7.7. For host nation-owned nuclear weapon systems, the host nation as Single Manager shall submit nuclear safety design certification documentation through Air Armament Center/Nuclear Weapons Directorate European Liaison Office (OL-EL/ELO). For foreign manufactured non-specialized equipment, whether U.S. or host nation-owned, the organization shall submit nuclear safety design certification documentation through OL-EL/ELO. OL-EL/ELO will serve as the interface between the host nation and the USAF on all nuclear safety design certification processes and issues.

8. Certification Process for Nuclear Safety Design Certified Technical Order Procedures. The certification process for technical orders is delineated in AFI 63-125, *Nuclear Certification Program*.

8.1. HQ AFSC/SEW approves new or major changes to ICBM OPCERT/DECERT procedures for critical components. AAC/NW approves minor changes to OPCERT/DECERT procedures. These procedures must adequately verify that the system or component functions as design certified and mitigates all credible threats and scenarios.

9. Critical Components. For certification of critical components, the organization with program management responsibility:

9.1. Initiates the design certification process for hardware and software.

9.2. Provides for a nuclear safety cross-check analysis (NSCCA) or independent validation and verification (IV&V) of software critical components according to **Attachment 2**, paragraph **A2.4.**

9.3. Develops OPCERT and DECERT procedures for hardware critical components and sends the procedures to HQ AFSC/SEW for approval.

10. Tamper Detection Indicators (TDIs).

10.1. For certification of TDIs, the operational MAJCOM or Single Manager determines the need for TDI application and sends a request to HQ AFSC/SEW that:

10.1.1. Identifies the critical component requiring a TDI.

10.1.2. Justifies why a TDI is needed.

10.1.3. States whether the TDI will be used in an operational system or a nonoperational environment for storage and transportation.

10.2. HQ AFSC/SEW evaluates the TDI application request and sends the approved application to the National Security Agency (NSA) for development of a suitable TDI.

10.3. By agreement, the NSA:

10.3.1. Develops the appropriate TDI based on the parameters and intended-use data provided by the operational MAJCOM.

10.3.2. Coordinates TDI development with the organization having program management responsibility.

10.3.3. Sends the TDI data required for application, control, storage, and inspection procedures to HQ AFSC/SEW for certification.

10.4. The requesting MAJCOM maintains responsibility for all procurement actions and costs associated with TDI development and integration.

10.5. Upon approval of the application, the Single Manager provides the technical requirements to the NSA and develops the nuclear surety evaluation required to obtain certification.

11. Special Test and Maintenance Programs.

11.1. The Single Manager must evaluate all aspects of the proposed program(s) for potential nuclear surety degradation. This evaluation includes conditions that could violate AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*, degrade existing safety and security features, or contribute to UL scenarios.

11.2. The Single Manager provides this evaluation and requests approval of the proposed program(s) from HQ AFSC/SEW.

11.3. HQ AFSC/SEW bases the approval decision on the findings of the evaluation and an independent review of the proposed program(s) (if required). A special safety study may also be required

according to AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules*.

12. Nuclear Weapon Maintenance or Test Procedures.

12.1. AF safety evaluation/review is required for all new or revised nuclear weapon maintenance or test procedures in relation to the facility where they are to be performed.

12.2. HQ AFSC/SEW must approve implementation of certain new or revised nuclear weapon maintenance or test procedures that will be accomplished in Air Force facilities. The qualifying programs are:

12.2.1. Programs to accomplish warhead ALTs and MODs.

12.2.2. Any programs that require bypassing or disabling any weapon safety features.

12.2.3. Procedures that introduce new or significant potential safety hazards, e.g., sources of electrical energy, fire hazards, etc.

12.3. AFNWCA must notify AFSC/SEW of weapon ALTs or MODs. AAC/NWL must notify AFSC/SEW and AFNWCA of any other new or revised maintenance or test procedures described in **12.2.2.** or **12.2.3.** above.

12.3.1. The notification via a Statement of Intent (SOI) will initiate an AF safety review/evaluation of the proposed procedures in relation to the facility where they are to be performed and must:

12.3.1.1. Provide background information and a description of the maintenance action to be performed.

12.3.1.2. Identify proposed temporary removal, bypass, or disablement of the surety features of the weapon itself.

12.3.1.3. Specify the Air Force facility where the procedures will be performed.

12.4. For Product Change Proposals (PCPs), submit the notification (SOI) no later than 180 days prior to scheduled maintenance. For Special Procedures (SPs) and Retrofit Orders (ROs), submit the notification when it is distributed for Air Force review/coordination.

12.5. AFSC approval (via formal documentation) must be obtained prior to implementation of procedures described in **12.2.** above.

12.6. Other nuclear weapon maintenance procedures (those not meeting the requirements of paragraph **12.2.** above) require AAC/NW safety evaluation but do not require formal AFSC approval.

13. Nonspecialized Equipment. Any equipment used with nuclear weapons but not specifically designed for that purpose is considered nonspecialized equipment, specifically items listed in paragraphs **4.4.** through **4.4.6.2.** Certain modifications to nonspecialized equipment do not require formal nuclear safety design certification. These modifications include:

13.1. Common add-on equipment such as fire extinguishers, radios, lights, bedliners, camper shells, sirens, foreign object damage (FOD) magnets or containers.

13.2. Minor field-level modifications to vehicles or AGE that do not impact the braking, steering, lifting, powertrain, or load carrying/restraint systems.

13.3. The following process should be used to determine the appropriate course of action for evaluation and local approval of minor field-level modifications.

13.3.1. Identify item(s) to be modified and provide a complete description of the proposed changes to the item Maintenance Supervisor/Superintendent (or equivalent) and the Unit Safety Office.

13.3.2. These offices will jointly review the proposed modification to determine if approval can be granted at the unit level or if further evaluation of the nuclear safety impact is necessary.

13.3.2.1. If there is no impact to nuclear surety, approve the modification locally.

13.3.2.2. If further evaluation is required, submit a formal request for evaluation/approval from the operational MAJCOM's safety office.

13.3.3. If formal nuclear safety design certification is not required, the operational MAJCOM will:

13.3.3.1. Provide formal approval to the field unit.

13.3.3.2. Inform the item manager and HQ AFSC/SEW of the approved modification.

13.3.4. If the modification requires formal nuclear safety design certification, the operational MAJCOM will:

13.3.4.1. Notify the submitter that further evaluation is necessary.

13.3.4.2. Follow the process specified in paragraph **7.**

13.3.5. For host nation-owned non-specialized equipment, the host nation as Single Manager shall submit certification documentation through OL-EL/ELO. OL-EL/ELO will serve as the interface between the host nation and the USAF on all nuclear safety certification processes and issues.

14. Lifting and Suspension Systems.

14.1. The lead/using command performs a nuclear surety evaluation and sends a certification request to HQ AFSC/SEW according to paragraph **7.4.**

14.2. A design or civil engineering agency evaluates the facility that will support the lifting or suspension system to determine if the structure meets the design requirements in AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon System*s. This evaluation and an appropriate analysis that the structure is safe for the rated load and meets the required margins of safety according to AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon System*s, must be included with the lead/using command's NSE.

14.3. An inspection and maintenance cycle for each certified facility lifting system will be established according to AFOSH Standard 91-46, *Materials Handling and Support Equipmen*t.

14.4. The lead/using command is authorized to use suspended load-frame assemblies at 100 percent of their rated load. These assemblies do not require periodic load testing but must be periodically inspected.

14.5. The lead/using command evaluates item or facility support structure modifications to determine their impact on the certification status.

14.6. HQ AFSC/SEW nuclear safety design certifies the facility lifting system and notifies AAC/NWC of the certification action so an update to the MNCL can be accomplished.

Section D—Decertification Process

15. Design Decertification.

15.1. HQ AFSC/SEW may remove nuclear safety design certification for items that have demonstrated inadequate safety through analysis, testing, or operational performance.

15.2. Any Air Force agency may send a recommendation for removal of nuclear safety design certification to HQ AFSC/SEW. The recommendation must identify the item as listed in the MNCL and include documentation that supports the recommendation.

15.3. Removal of nuclear safety design certification is done via a formal notification letter from HQ AFSC/SEW to AAC/NWC.

15.4. A nuclear safety design certified item may be restricted from use with nuclear weapons at any time and for any reason (e.g., damage, modifications, or changes to intended usage, etc.). Such restrictions do not constitute removal of nuclear safety design certification. However, appropriate documentation in historical or permanent records is required to preclude inadvertent use. If desired, submit a request to AFSC/SEW to restrict specific item(s) from use and AFSC/SEW will notify AAC/NWC to annotate the MNCL accordingly.

16. Operational Decertification.

16.1. Critical components or systems that have been improperly stored or not maintained according to AFI 91-105, *Critical Components*, require decertification if the resulting mishap investigation does not positively rule out tampering. Decertification is also required if a critical component is connected to an uncertified interface (i.e., not certified via OPCERT procedures or through nuclear safety design certification approval as documented in this publication).

16.2. Operational MAJCOMs may decertify critical components if they use approved decertification procedures (when applicable) and the intended life cycle for the critical component does not specifically prohibit decertification.

MAURICE L. McFANN, JR., Major General, USAF
Chief of Safety

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

GOVERNMENT REFERENCES

DOD 3150.2-M, *DoD Nuclear Weapon System Safety Program Manual*

DOD Guidelines for Software Development

DOD/DOE Procedural Guideline for the Phase 6.X Process

Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*

USAF REFERENCES

AFPD 37-1, *Information Management*

AFMAN 37-123, *Management of Records*

AFPD 91-1, *Nuclear Weapons and Systems Surety*

AFI 91-101, *Air Force Nuclear Weapons Surety Program*

AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules*

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

AFI 91-105, *Critical Components*

AFI 91-106, *Unauthorized Launch and Launch Action Studies*

AFI 91-107, *Design, Evaluation, Troubleshooting and Maintenance Criteria for Nuclear Weapon Systems*

AFI 91-204, *Safety Investigations and Reports*

AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems*

AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems Software*

AFMAN 91-221, *Weapons Safety Investigations and Reports*

AFPD 63-1, *Capability-Based Acquisition System*

AFI 63-125*, Nuclear Certification Program*

AFI 63-1201*, Assurance of Operational Safety, Suitability and Effectiveness*

AFPAM 63-126, *Nuclear Certification Process*

Air Force Records Disposition Schedule (RDS) located at **https://webrims.amc.af.mil**

Abbreviations and Acronyms

AAC/NW—Air Armament Center/ Nuclear Weapons Directorate

AAC/NWC—AAC/NW Certification Management Division

AFI—Air Force Instruction

AFNWCA—Air Force Nuclear Weapons and Counterproliferation Agency

AFSC—Air Force Safety Center

AFSC/SEW—AFSC, Weapons Safety Division

AFSC/SEWN—AFSC/SEW, Nuclear Weapons Branch

AFTO—Air Force Technical Order

ALT—Alteration

CRP—Certification Requirements Plan

DECERT—Operational Decertification

DOD—Department of Defense

ELO—European Liaison Office

FOD—Foreign Object Damage

HQ AFSC—Headquarters, AFSC

IV&V—independent validation and verification

MAJCOM—major command

MNCL—master nuclear certification list

MOD—modification

NCIS—nuclear certification impact statement

NCM—nuclear certification manager

NSA—National Security Agency

NSAR—Nuclear Safety Analysis Report

NSCCA—Nuclear Safety Cross-Check Analysis

NSE—Nuclear Surety Evaluation

NSP—Nuclear Surety Procedures

OPCERT—Operational Certification

PCP—Product Change Proposal

TDI—Tamper Detection Indicator

TNSA—Technical Nuclear Safety Analysis

TO—Technical Order

TOMA—Technical Order Management Agency

UL—Unauthorized Launch

Terms

Single Manager—The single individual specifically designated, under the integrated weapon system management architecture, to be responsible for the life cycle management of a system or end-item. The Single Manager is the program manager vested with full authority, responsibility, and resources to execute and support an approved Air Force program. For facilities, the SM is the operational MAJCOM vested with life cycle management and configuration control responsibility for the facility.

Attachment 2

GROUPS, SAFETY ANALYSES, PLANS, EVALUATIONS, AND REVIEWS

A2.1. Nuclear Surety Working Group (ICBMs) and Nuclear Weapon Delivery System Project Officer Groups:

A2.1.1. For ground-launched missile systems, a nuclear surety working group is used to coordinate nuclear surety requirements among the various agencies involved in nuclear certification.

A2.1.2. For aircraft and air-launched missile systems, a delivery systems project officer's group is used to coordinate nuclear certification issues.

A2.2. Nuclear Surety Evaluation (NSE). Evaluates items to be nuclear safety design certified using the approved certification approach (as identified in the CRP). The NSE focuses on all AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems,* design and evaluation criteria applicable to the item. It includes a recommendation for certification or certification with restrictions (to meet AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*).

A2.3. Independent Nuclear Surety Review. The independent nuclear surety review:

A2.3.1. Is of sufficient depth to ensure the nuclear surety evaluation is technically correct and complete.

A2.3.2. Specifically addresses the design requirements.

A2.3.3. Indicates if the design meets AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*.

A2.3.4. When requirements are not met, the review must include comments and documentation on the adequacy of compensatory measures and specify if the reviewing agency concurs with the evaluating agency's recommendation for nuclear safety design certification.

A2.3.5. For host-nation procured support equipment, the independent nuclear surety review is conducted internally during the NSE development process conducted by OL-EL/ELO.

A2.4. Software Evaluations. Nuclear critical software evaluation can be accomplished by Nuclear Safety Cross-Check Analysis (NSCCA) or Independent Validation and Verification (IV&V). Nuclear safety design certified software can be evaluated by IV&V or other Quality Assurance analyses as delineated in the CRP. AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems Software,* provides guidelines for determining the method of and criteria for evaluation. Requirements for software evaluation can range from full NSCCA to qualification testing depending on the relationship to critical functions (authorization, prearming, launching, releasing, arming, and targeting). Additional factors include the potential for unauthorized launch threats and scenarios. Although these evaluations use many similar techniques, they are typically performed by different organizations, have different objectives, and produce different results. NSCCA and IV&V are performed by an organization technically, managerially, and financially independent of the developer. HQ AFSC/SEW will make the final determination regarding independency requirements.

A2.4.1. An NSCCA has the single objective of ensuring that the program cannot perform in any way that could contribute to a nuclear safety violation. Analysis and testing focus on ensuring that nuclear safety-critical functions are performed correctly and that the program does not perform any unintended functions that could violate nuclear safety. The NSCCA is also unique in its concern for sabotage. While the other forms of software evaluation assume that any program deficiencies will be unintentional, the NSCCA also looks for intentionally caused problems and employs special security and control measures to prevent sabotage of the NSCCA effort itself. An NSCCA begins with the development of nuclear safety objectives (NSOs) and nuclear safety requirements (NSRs). NSOs represent the overall objectives a nuclear weapon system must satisfy in order to obtain nuclear safety certification. NSRs form the basis for all subsequent NSCCA activities. A traceability analysis is performed to demonstrate that all NSOs are represented in the NSRs and that all NSRs are derived from one or more NSOs. The NSCCA is completed by conducting a bit-for-bit comparison (under the Two-Person Concept) between the software delivered to the operational MAJCOM and the software analyzed by the NSCCA organization.

A2.4.2. Independent Validation and Verification (IV&V). IV&V is a software evaluation process that includes both analysis and testing and extends throughout program development. “Verification” analyzes software requirements, design, and code to detect program deficiencies before they can propagate into later development phases. “Validation” analyzes and tests the final program to determine its compliance with requirements. IV&V is distinguished from qualification testing by its emphasis on detecting program weaknesses and unforeseen circumstances that the program will be unable to handle. **Attachment 3** provides a generic IV&V program plan to define the approach used by the IV&V contractor/evaluation team in support of software nuclear safety design certification.

Attachment 3

GENERIC INDEPENDENT VALIDATION AND VERIFICATION (IV&V) PROGRAM PLAN

A3.1. Purpose. The purpose of this program plan is to define the approach to be used by the IV&V contractor/evaluation team in support of nuclear safety design certification of the software/firmware in question. The overall nuclear safety design certification effort is defined in another program plan. Nuclear certification of software/firmware is one of the positive measures the Air Force uses to assure that the software/firmware, as designed, coded, and implemented, complies with the DOD Nuclear Weapon System Safety Standards (DOD Directive 3150.2, *Safety Studies and Reviews of Nuclear Weapon Systems*) and meets the safety design and evaluation criteria for nuclear weapon systems in AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*.

A3.2. Equipment/System Description. This section provides a brief description of the weapon system that will allow the reader to understand the functional and nuclear safety implications of the weapon system. Where individual software/firmware pieces are involved, provide a brief description of each item at the block diagram level. A brief description includes performance requirements and software/firmware design showing correlation to requirements and stressing features that provide nuclear surety.

A3.3. IV&V Concepts.

A3.3.1. Validation is defined as the test and evaluation process that ensures the software/firmware meets all system and software performance requirements; verification is the repetitive process for ensuring that, during each development phase, the software/firmware satisfies and implements only those requirements approved at the end of the previous phase. For the purpose of nuclear safety, the validation and verification effort has primary emphasis placed on the nuclear safety issues identified below. Using an independent contractor to perform this task adds an additional layer of confidence and security to the process.

A3.3.2. The IV&V effort will concentrate on the software/firmware functions that must be verified to obtain nuclear safety design certification in accordance with this AFI. The key step in this effort is identifying the nuclear safety contributions and how the software/firmware could possibly impact or affect the weapon system nuclear critical functions as defined in AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems*. These critical functions are: authorization, launching/releasing, warhead prearming/arming, and targeting. All of the software/firmware functions and capabilities will be evaluated to determine the level and extent of their contributions, resulting in nuclear safety impacts to the above critical functions. Contributions that cause a possible degradation of nuclear safety or performance will be reported as discrepancies for program office evaluation.

A3.3.3. All nuclear safety discrepancies will be identified, evaluated, and prioritized according to their potential impact on nuclear safety. A priority scheme is used to evaluate nuclear safety discrepancies and determine their impact on nuclear safety (Critical, Urgent, Degraded, Noncritical, Minor).

A3.3.4. The results obtained from the IV&V effort will be included in the final IV&V report and will also be used in the preparation of the demonstration test plan and Nuclear Surety Evaluation (NSE) report. Inputs will also be made to the qualification demonstration and data will be examined from those tests with regard to verification of the software/firmware. Finally, the data from these efforts

will be maintained in a database at the program office to support future modifications and technical order updates.

A3.4. IV&V Approach. This section describes the specific approach that will be taken to conduct the IV&V effort.

A3.4.1. Test Plan. The IV&V contractor designs and conducts tests to verify the software/firmware design complies with AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*. This test approach is detailed in the IV&V Test Plan.

A3.4.2. Configuration Control. The program office will maintain configuration control. This task may be contracted out, but the ultimate responsibility for configuration control remains with the single manager. Discrepancy reports will address performance as well as nuclear safety aspects of the software/firmware functions and capabilities. These reports will provide all pertinent information (such as problem areas, descriptions, impacts, and recommendations) required to pursue appropriate action.

A3.4.3. Analysis Tools. In order to implement the IV&V approach effectively, specific analysis tools may be developed to perform both the tracing studies and the software/firmware checkout. The analysis tools themselves will be validated to the degree required to ensure accuracy and completeness.

A3.4.4. AFI Compliance. AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*, and AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon System Software,* will be used to guide and direct the IV&V efforts. Particular attention will be given to memory organization, fault detection/handling capabilities, and the adequacy of self-test circuitry. A summary table should show compliance and the specific analysis or demonstration efforts.

A3.4.5. Source Code Testing. The source code is checked for implementation, using the Computer Program Development Specification and the Computer Program Product Specification. Items that will be checked are the code structure, decision/branch points, input/output handling, and module coupling. The test plan outlines the steps to check the source code at both the modular and/or functional level for those areas impacting nuclear safety. A “test requirements" checklist versus a "test approach" checklist will be generated to determine how functions will be verified. A "master procedures" checklist will be constructed to identify which tests are exercised for each module (or logical group of modules). The tests will be a combination of manual analysis and development site testing.

A3.4.6. Test Results Report. A test results report will discuss the software/firmware code checkout effort. Summary result tables will be provided. All discrepancy reports and their resolution will be included.

A3.4.7. Object Code Testing. Once the source code is checked, it will be compiled into an executable object code. For ground-launched missile systems, a bit-by-bit compare against the object code delivered by the development contractor will be accomplished. Differences will be identified and explained. Discrepancies will be documented and resolution recommended.

A3.4.8. Final Report. A final report will include IV&V results. The report will evaluate whether the software/firmware satisfies AFI 91-107 *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*, design standards and, via the discrepancy reports, will identify any known nuclear safety concerns. Each discrepancy report will have an evaluation and recommendation. The report will conclude with a recommendation on nuclear safety design certification. The report will be included as part of the Nuclear Surety Evaluation (NSE).

A3.5. Schedules. Significant milestones are submittal/approval of IV&V Program Plan, IV&V Test Plan, Final IV&V Report, and the NSE report. The first two items are especially critical to the success of IV&V.

Attachment 4

RECOMMENDED OUTLINE FOR THE NUCLEAR SURETY EVALUATION (NSE)

A4.1. Certification Action. Recommend certification or certification with restrictions (to meet AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*).

A4.2. Item Identification. For hardware or software (as applicable) provide:

A4.2.1. Nomenclature or common name.

A4.2.2. National item identification number.

A4.2.3. Manufacturer and code.

A4.2.4. Model and part number.

A4.2.5. Computer program identification number.

A4.2.6. Item manager (include the functional address symbol and telephone number).

A4.3. Uses and Description. Provide information on:

A4.3.1. Equipment uses.

A4.3.2. Weapons.

A4.3.3. Weapon types (as considered in the analysis).

A4.3.4. Top-level description.

A4.4. Summary of Engineering Analysis (Evaluation and Test):

A4.4.1. Identify the specific AFI 91-107, *Design, Evaluation, Troubleshooting, and Maintenance Criteria for Nuclear Weapon Systems*, AFMAN 91-118, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems,* and/or AFMAN 91-119, *Safety Design and Evaluation Criteria for Nuclear Weapon Systems Software,* criteria used in the design and evaluation process for the item.

A4.4.2. Discuss the certification approach used (compliance verification methods).

A4.4.3. Identify or reference the specific test and analysis procedures used.

A4.4.4. Summarize the results of the certification analysis, and discuss any discrepancies identified during the evaluation and their disposition.

A4.5. Recommended Restrictions. Recommend any restrictions needed to compensate for uncorrected design deficiencies or discrepancies.