BY ORDER OF THE SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 91-106

23 NOVEMBER 1993

Safety

UNAUTHORIZED LAUNCH AND LAUNCH ACTION STUDIES

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 122-6, 19 January 1987

Pages: 16

Distribution: F

This instruction implements AFPD 91-1, *Nuclear Weapons and Systems Surety*. It provides guidance for conducting an unauthorized launch study (ULS) and a launch action study (LAS); prepare, distribute, control, and use ULS and LAS reports; and imposes assignment limitations on persons who had access to the reports or data. This applies to all organizations that design, develop, modify, test, evaluate, or operate ground-launched missile nuclear weapon systems. It does not apply to US Air Force Reserve and Air National Guard units and members. Send major command (MAJCOM) supplements to this instruction 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 revision aligns the instruction with AFPD 91-1; incorporates the requirements and procedures formerly in AFR 122-6; cross-references the list of terms and definitions in the 91-1 series Air Force directives; adds guidance for LASs; includes the responsibilities of the Air Force Chief of Safety; and adds unauthorized launch scenario evaluation guidelines and criteria.

Section A—General Information

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

2. Air Force Goal. The Air Force studies each new or significantly modified ground-launched missile nuclear weapon system to determine the likelihood of an unauthorized launch (UL) and pinpoint countermeasures to UL threats. These measures implement the Department of Defense (DoD) Nuclear Weapon System Safety Standard requiring each Military Service to provide safeguards that will prevent deliberate UL of a nuclear weapon.

3. Purpose of ULSs and LASs:

3.1. Purpose of a ULS. Conduct a ULS to identify vulnerable areas in a system that an agent or agents could exploit in a covert or overt fashion to bypass the nuclear safety and security features of a ground-launched missile system. These vulnerabilities could allow the UL of a missile using its own propulsion subsystem. A ULS suggests ways that you can neutralize these vulnerabilities.

3.1.1. The ULS report becomes a source document that you can use to develop a technical nuclear safety analysis (TNSA), and to assess the adequacy of the system safety design, system modification, or system security features. The TNSA supports safety studies and helps develop nuclear weapon system safety rules according to AFI 91-102, *Nuclear Weapon System Safety Studies, Operational Safety Reviews, and Safety Rules* (formerly AFR 122-2). If you fail to prepare a satisfactory ULS report, you may delay weapon system deployment or modification.

3.1.2. Addendum ULS Report. An addendum ULS report complements or adds to the basic ULS report. You can do an addendum ULS when you add a new capability to a nuclear weapon system, or when you identify a new threat to an existing weapon system. Do not do an addendum report if the basic ULS report is outdated, or if the resulting addendum report conflicts with the basic report. A ULS report is outdated when a technological advance poses a threat not identified in the basic report, or changes the threats or UL scenarios. When you prepare an addendum:

- Identify all the documents you use in the addendum.
- Identify the basic report and documents that the addendum affects.
- Provide an addendum number, publication date, and description of the weapon system change that made the addendum necessary.

3.1.3. The launch activation path (LAP) diagram illustrates actions and processes associated with weapon system authorization and launch functions. You may need many such diagrams for a single ULS. Examine all diagrams to determine the relationship between weapon system authorization and launch critical functions, and weapon system components. Based on the LAP, identify weapon system components that are likely targets for attack. Conduct an LAS for each component you identify.

3.2. Purpose of an LAS. An LAS is a limited-scope study that a full-scale development (FSD) contractor or Air Force agency completes. The LAS identifies threats that FSD systems or components introduce into weapon systems. The study analyzes these threats without adding or relying on mitigating external factors of the analyzed component.

Section B—General Responsibilities

4. Air Force Chief of Safety (HQ USAF/SE). HQ USAF/SE establishes requirements to conduct ULSs of new or significantly modified ground-launched missile weapon systems. Acting for HQ USAF/SE, the Commander, Air Force Safety Agency, manages the process and directs HQ AFSA/SEN to:

- Determine when a basic report is outdated and requires revision.
- After identifying a ULS requirement, determine if a revision or an addendum is appropriate.
- Keep the master file of all ULSs.
- Determine if a weapon system modification warrants a ULS.
- Keep the master file, of assignment limitations.

- Determine and controls distribution for all ULS and LAS reports.
- Control ULS and LAS report transfer, reproduction, and destruction.
- Approve credible UL scenarios and mitigation requirements when a safety study (conducted according to AFI 91-102) is unnecessary.

5. Nuclear Weapon System Safety Group (NWSSG):

- Reviews ULS reports, if any, prepared for the weapon system under study.
- Identifies components for critical component consideration, as defined in AFI 91-105 (formerly AFR 122-17), *Critical Components*.
- Recommends ways to mitigate or correct credible UL scenarios.

6. Operational Commands and Affected Agencies:

- Control ULS and LAS reports in their possession, according to this instruction.
- Limit access to ULS reports and data to essential personnel to avoid imposing excessive assignment limitations.
- Appoint an access-granting official.
- Notify personnel (in writing) of assignment limitations after exposure to ULS information.

7. Engineering Command or Agency. The command or agency responsible for procuring or modifying a nuclear weapon system must:

- Notify HQ AFSA/SEN of weapon system modifications that impact current critical components, or are relevant ULS candidates, according to past ULSs.
- Conduct ULSs, addendum ULSs, and LASs and publishes reports for weapon systems under its responsibility.
- Maintain the master copy for each ULS report that the command publishes.
- Control ULS and LAS reports according to this instruction.
- Appoint an access-granting official.
- Notify personnel (in writing) of assignment limitations after exposure to ULS information.
- Chair the ULS Steering Committee.

Section C—Conducting Studies and Preparing Reports

8. Conducting a ULS:

8.1. Assessing Susceptibilities. The ULS requires an analysis and a report. You must conduct the analysis in parallel with the design and development effort to recognize and minimize the likelihood of UL before weapon system production or modification. Use the LASs as the first tools of the analysis. Begin no later than the preliminary design review to provide sufficient information to the ULS team for early UL susceptibility assessment. For both hardware and software modifications, the final ULS report must arrive in time to support the engineering evaluation according to AFI 91-103, *Air Force Nuclear Safety Certification Program* (formerly AFR 122-3) , or the TNSA according to AFI 91-102. Apply the following guidelines:

- Provide a ULS progress report (including candidate critical components) to HQ AFSA/SEN 30 calendar days before the critical design review (CDR). You do not need a progress report if you send the draft ULS report 30 calendar days before the CDR.
- Provide a draft ULS report to HQ AFSA/SEN 120 calendar days before the required certification need date, or the NWSSG study date.
- Provide the final ULS report to HQ AFSA/SEN 60 calendar days before the required certification date, or the NWSSG study date.
- Conduct LASs early enough to meet ULS report schedules.

8.2. Contracting Studies:

8.2.1. The engineering command can contract for a ULS, including LASs. The command must not contract the ULS to the contractor who is developing the system or modification.

8.2.2. The command will not divulge previous ULSs, analyses, or data, to prospective bidders.

8.2.3. After being awarded the contract, the contractor can access appropriate existing ULSs.

8.2.4. The contractor must comply with all access and control requirements.

8.2.5. The engineering command ensures that the ULS and LAS meet the applicable requirements of this instruction.

8.3. Study Team:

8.3.1. The engineering command should establish a ULS team to conduct the study, or require a ULS team as part of the study contract.

8.3.2. Include experts in all the disciplines affected by the system development or modification, such as hardware, software, systems integration, safety, security, and communications security. The size of the team depends on the extent of the project and expertise needed.

8.4. Outside Agency Participation. Include in the ULS team qualified experts who can analyze all system operations and functions.

8.4.1. If required, include experts from outside agencies (National Security Agency, other engineering agencies, operational commands, contractors, or other agencies with unique capabilities) as part of the ULS team.

8.4.2. Operational commands must participate to ensure that the study considers operations and maintenance procedures and to alert the command to potential threats to the weapon system.

8.5. ULS Steering Committee. The engineering command chairs this committee. The committee:

- Includes representatives from the engineering and operational commands, the independent review agency designated by the Air Force Materiel Command, the National Security Agency, and HQ AFSA/SEN.
- Ensures that each threat and scenario complies with the assumptions, ground rules, and rating guidelines in paragraph **9.**
- Helps establish the technology and threat baseline for the ULS.
- Adjusts individual step and scenario ratings to include information that the ULS contractor has not considered.

- Ranks all scenarios that fall within the same rating category.

9. Analyzing the UL Threat:

9.1. Assumptions. A scenario is a complete path of necessary launch actions required to complete missile launch. Construct threats and scenarios based on the following assumptions:

- A given scenario involves only one cognizant agent, but can employ any number of third-party agents (with or without cognizant agent support).
- If the technology exists, the cognizant agent, or at least one third-party agent, has the knowledge and capability to complete the threat or scenario.
- A cognizant agent knows the codes he or she has handled.
- Third-party agents do not have initial knowledge of secure codes (such as permissive action links, sealed authenticator systems, and enable or launch codes). However, they have or can get detailed system information, including classified data on the design, use of equipment, and the command and control structure.
- Technical orders are accurate and complete.
- Hardware, software, and firmware delivered to the operational command have no manufacturing defects that could contribute to a UL, and are certified according to AFI 91-103.
- The UL attack is covert until the agent successfully completes all required actions overtly.

9.2. Ground Rules for UL Threat Analysis:

9.2.1. Consider the operational unit the primary target for UL actions. Examine possible actions originating outside the operational unit, such as during transportation, or at contractor facilities, maintenance and support depots, and supply facilities.

9.2.2. When you first develop launch action threats or UL scenarios, disregard procedural safeguards, such as split-handling, split-knowledge, and Two-Person Concept controls. Air Force instructions, nuclear weapon system safety rules, or HQ AFSA/SEN apply safeguards as needed to help mitigate UL scenarios.

9.2.3. Assume that a cognizant agent can conduct covert actions using tools normally present at the site, or can carry in any other tools or devices without creating suspicion. The agent can also use:

- Planned support or previously positioned tools.
- Heavy construction equipment, tools, or weapons for UL attempts involving forced entry into secure facilities.

10. Preparing a ULS Report. Use the following outline to prepare the final ULS report:

10.1. Introduction. Identify the ULS scope and purpose, including assumptions, ground rules, methodologies, limitations, and applicable documents.

10.2. Executive Summary. Present a top-level logic tree of the entire ULS, top-level LAPs, as well as summaries and rankings of the various UL scenarios.

10.3. Weapon System Description. Include an abbreviated summary with diagrams, flow charts, and LAP descriptions.

10.4. Analysis. Provide UL scenarios, applicable procedures, and security requirements:

10.4.1. Identify in the LAP all system components that an agent can compromise or alter to cause a UL.

10.4.2. Conduct LASs to define launch action threats against the system components identified in the LAP.

10.4.3. Use the LASs to describe components and their functions for each launch action threat:

- Indicate agent preparations and attack procedures at each susceptible location in the component's life cycle.
- Estimate the time needed to execute the launch action threat.
- Identify tools and equipment needed to carry out the launch action threat.
- Estimate the time needed to detect the launch action threat.
- Identify methods to counter the launch action threat.
- Estimate the time needed to counter the launch action threat.

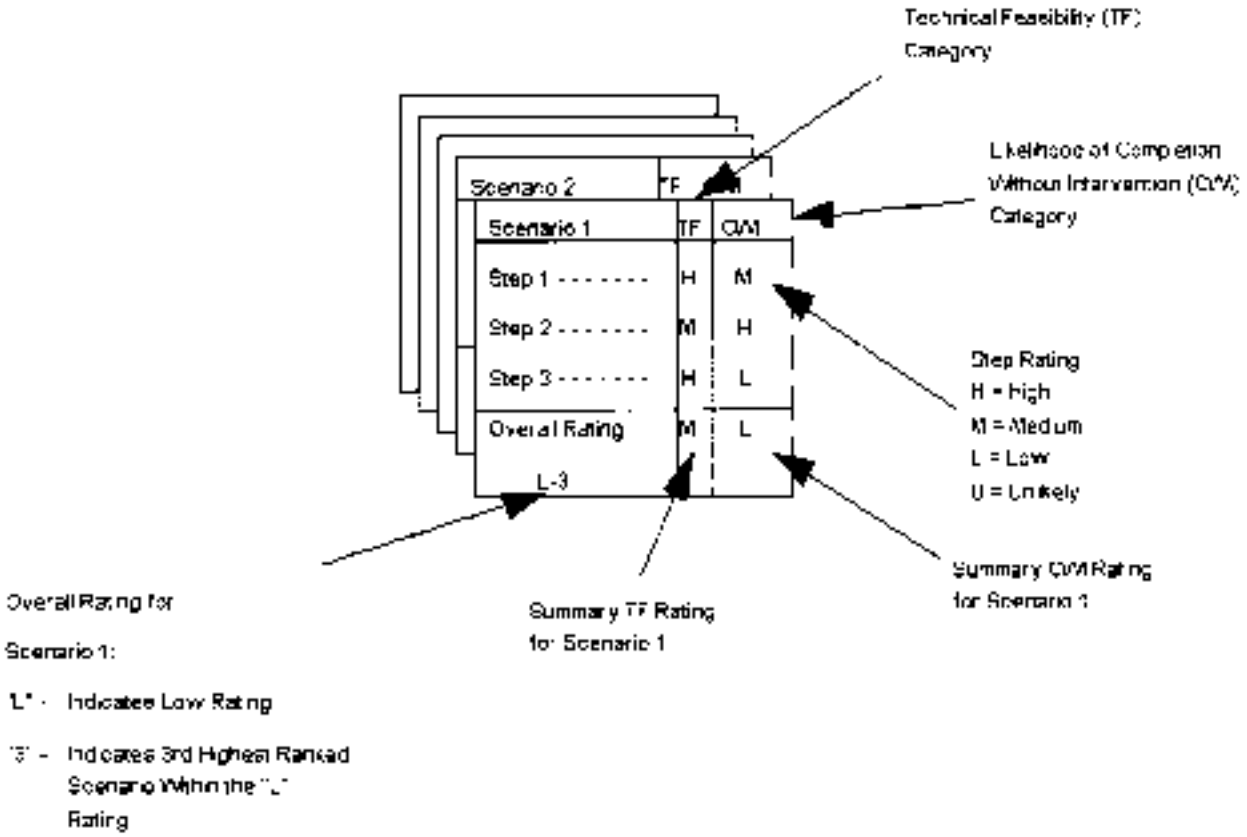
10.4.4. Use the LAP as a guide to organize and format the various launch action threats into credible UL scenarios, as follows:

- Provide sequential description of each scenario, including the type of launch that could result. (See AFI 91-101, *Air Force Nuclear Weapons Surety Program* for definitions of launch types 0, 1, 2, and 3.)
- Estimate the time needed to execute each scenario.
- Identify tools and equipment needed to carry out each scenario.
- Estimate the time needed to detect the UL attempt.
- Identify methods to counter each UL scenario.
- Estimate the time needed to counter the UL attempt.
- Indicate characteristics of missile support equipment, computer software, security systems, and other features and procedures that let defending forces detect and stop the UL attempt.

11. UL Scenario Evaluation Guidelines and Criteria:

11.1. UL Scenario Evaluation. Sort the scenarios into initial technical feasibility (TF) and completion without intervention (CWI) groups before you apply any mitigating factors. Rank UL scenarios to determine which scenarios are the most likely to occur. When you later apply mitigating factors, adjust the TF and CWI assignments accordingly and re-rank the scenarios. This process assesses the effectiveness of each mitigating factor and forms the basis for a recommended set of mitigating factors. **Figure 1.** illustrates a typical UL scenario format.

Figure 1. Typical UL Scenario



11.2. **Creating a Typical Scenario.**

- Assign each step a rating of High, Medium, Low, or Unlikely.
- Determine a summary rating for the TF and CWI categories based on the ratings of individual steps.
- Assign an overall rating to each scenario. Rank scenarios within each rating group.

11.3. Evaluation Categories. Use TF and CWI evaluation categories as described below.

11.3.1. TF Category. The TF rating indicates current availability of technology and resources needed to perform the scenario step.

Step 1. Assess how hard it would be to complete the step. Addressing factors such as the likelihood of successful integration of complex design changes with an operational system without testing the entire system under realistic conditions.

Step 2. Assume the agent knows, or can learn how to use the technology. Assume also that the agent has, or can acquire, currently available resources or technology; and that he or she can assemble the resources, and perform the technical activities to complete the step.

Step 3. Assign ratings as follows:

- *High*. The technology and resources to perform the step exist. The work requires no system-level simulation or testing.
- *Medium*. The technology and resources to perform the step exist. Successful system interface requires low or moderate system simulation or testing.
- *Low*. The technology and resources needed to perform the step exist. Successful system integration will require high fidelity system-level simulation or testing is needed to ensure a successful system interface; or a high risk of failure exists due to either unproved technology or the high degree of complexity needed to implement the threat.
- *Unlikely*. To complete the step, one or both of the following conditions apply:

- The technology to perform the step is unproved, or not yet developed.
- You cannot make the final adjustments to ensure interface compatibility until you complete actual connections to the operational system.

11.3.2. CWI Category. Use the CWI rating to indicate the agent's ability to successfully complete the step without detection or intervention.

Step 1. When you use CWI, consider the time the agent would need to complete the step, versus the "window of opportunity" that would be available to the agent. Also consider the levels and types of security the agent must breach; as well as the physical availability of the resources and technology.

Step 2. Evaluate the possibility that weapon system hardware, software, or status will fail to identify the unauthorized action.

Step 3. Remember that large or awkward tools or equipment increase risk of detection, even when the agent does not breach a security system.

Step 4. Assign ratings as follows:

- *High*. The agent can complete the entire step without challenge or detection; or the weapon system hardware, software, or status will fail to identify the unauthorized action. Resources are readily available from common sources.
- *Medium*. To complete the step, one or more of these conditions must apply:

- The agent must bypass unmanned security features.
- The agent will need large or awkward tools or equipment.
- The agent will require either the same or less time than the security force response time.
- The system hardware, software, or status will probably fail to identify the unauthorized action.
- The resources are readily available, but only from a specialized source.

- *Low*. To complete the step, one or more of these conditions must apply:

- The agent must bypass manned security features (including the Two-Person Concept).
- The agent needs more time than the security force response time allows.
- System hardware, software, or status will probably identify the unauthorized action.
- The resources exist in an unproved or experimental state and the agent can get them only from a scientific research center.

- *Unlikely*. To complete the step, one or more of these conditions must apply:

- Intervention is certain.
- The agent needs much more time to complete the steps than the security force response time allows.
- System hardware, software, or status will identify the unauthorized action.
- The technology does not exist.

11.3.3. Summary Rating Guidelines. For each step in the TF and CWI categories, assign a rating of high, medium, low, or unlikely. Give a preliminary summary rating to the TF and CWI categories. Base the rating on the lowest rated step in the category. Other considerations may dictate assigning a higher rating. The ULS Steering Committee can adjust the final summary rating of the category.

11.4. Overall Scenario Ranking. Determine an overall rating for each scenario based on the TF and CWI summary ratings. Use the lower rating of the TF, or CWI summary rating. The ULS Steering Committee can adjust the rating to reflect factors that are not easily quantifiable.

11.5. Scenario Ranking Guidelines. After you assign the overall scenario ratings, the ULS Steering Committee must evaluate and compare scenarios, then rank them as High, Medium, or Low. The relative ranking in a rating is subjective, but you should consider the following factors:

- Consequences of successful scenario completion.
- Scenario TF and CWI ratings.
- TF and CWI ratings for individual steps.
- Number and independence of steps.
- Effectiveness of applied threat mitigation techniques.

11.6. Conclusions and Recommendations:

11.6.1. Arrange all identified UL scenarios in the order most likely to occur. Consider factors such as time required, ease of task, and availability of tools and equipment. Include a summary in which you explain why you believe the scenario is accurate.

11.6.2. Identify the location or locations most susceptible to a successful UL attempt.

11.6.3. Provide a list of candidate critical components.

11.6.4. Recommend measures, such as redesign, split-handling, split-knowledge, or Two-Person Concept control, that could counter each UL threat.

11.6.5. Identify duties that may require assignment limitations on personnel after their exposure to UL information.

11.6.6. Identify the information, by ULS report paragraph number, that requires assignment restrictions.

Section D—Study Report Controls

12. Information Controls and Safeguards:

12.1. Classification. Table 1. contains guidance for classifying ULS and LAS information.

12.2. Controlling Material. Agencies and contractors participating in the study and preparing the report must:

- Strictly control, safeguard, and properly mark all draft and final ULS and LAS manuscripts, reports, and report files.
- Emphasize and enforce strict control on a need-to-know basis.
- Limit the number of people participating in the study and report preparation.
- Distribute ULS and LAS data only to the ULS contractor, contracting agency, and Air Force agencies approved by HQ AFSA/SEN.
- Destroy all ULS and LAS working papers in an approved manner when you publish the final ULS report described in paragraph **10.**

12.3. ULS and LAS Final Documents:

12.3.1. HQ AFSA/SEN controls the distribution of ULS and LAS reports. All outside commands or agencies obtain prior approval from HQ AFSA/SEN for document distribution.

12.3.2. The engineering command that performs or contracts for the ULS keeps the master copy. If a contractor prepares the ULS report, the master copy, and all ULS data, transfer to the engineering command after the report is complete.

12.3.3. HQ AFSA/SEN determines the number of copies to produce, and defines the agency distribution list.

12.3.4. Place the following statement on the cover sheet of each document:

Distribution of, and access to, this document is limited by the Air Force Safety Agency (AFSA).

Send requests to distribute or reproduce any partof this document to HQ AFSA/SEN, 9700 Avenue G, Kirtland AFB NM 87117-5671, for approval. *WARNING:* Access to this document restricts individuals from certain assignments, according to section F of AFI 91-106, *Unauthorized Launch and Launch Action Studies*.

Table 1. Classification Guide for Unauthorized Launch and Launch Action Studies.

RULE	A If the information reveals	B then the classification is	C and it applies
1	a compilation of ULS scenarios for any weapon system covering multiple areas of vulnerabilities	Top Secret	to basic or revised studies for each weapon system configuration.
2	a single, complete ULS scenario with detailed procedures and timeliness		to each individual scenario.
3	a single or compilation of ULS scenarios limited to a single areasof vulnerability but revealing detailed procedures	Secret	during studies for modifications when an addendum is written.
4	partial ULS scenario or scenarios		during a ULS study preparation or briefing.
5	detailed procedures for accomplishing a portion of a ULS scenario and revealing a system vulnerability		to all documents containing detailed procedures.
6	a complete LAS with detailed procedures		
7	a partial LAS with detailed procedures		
8	a complete LAS without detailed procedure and revealing a component vulnerability	Confidential	
9	a partial LAS without detailed procedure and revealing a component vulnerability	Unclassified	to all LASs without detailed procedures.
10	the existence of ULSs and LASs		not applicable.
11	vulnerabilities to communications security keys, codes, or algorithms	Top Secret	to all systems using command and control--AFI 33-209 (formerly AFR 56-3).

13. Distribution or Single Access Requests:

13.1. Obtaining Reports. Agencies can request one-time access to a ULS report, or request a permanent copy of a ULS report.

13.2. Request Address. Send requests, with an explanation of why you need the report, to HQ AFSA/SEN for an evaluation on a need-to-know basis.

14. Transfer, Reproduction, and Destruction of ULS Reports:

- Do not transfer, reproduce, or destroy a ULS report without HQ AFSA/SEN approval.
- Mark, transfer, and destroy classified ULS reports according to AFPD 31-4 (formerly AFR 205-1), *Information Security.*
- Obtain HQ AFSA/SEN approval before you courier Top Secret ULS reports aboard a commercial aircraft.
- Place the following statement on the inner wrapper: "To be opened only by (name and office symbol)."
- You must prepare and seal the inner wrapper of the report under the direct control of a person authorized access to the ULS report.

Section E—Access Responsibility and Authority

15. Management Responsibility:

15.1. Sensitive Material. ULS reports are extremely sensitive, and because access to ULS reports and data limits a person's choice of assignments (see section F), you must manage them responsibly. This is particularly important in an operational MAJCOM and combatant command, since ULS reports identify specific UL actions that are likely to start in a command.

15.2. MAJCOM Obligations. Operational MAJCOMs:

- Grant access only to MAJCOM or combatant command headquarters staff members and key wing personnel (wing commander or the authorized representative) who establish policies and procedures to counter UL threats.
- Limit the ULS information that key wing personnel receive to the information they need to understand the specific threats they must recognize, and the actions they must take to counter those threats.

16. Access Authority:

16.1. DoD Custody. DoD agencies with custody of ULS reports appoint an individual and (optionally) an alternate, as the official who grants access. It is the appointed official's job to notify HQ AFSA/SEN of each appointment.

- The access-granting official authorizes access to ULS reports and briefings. The official prepares an access list to control access for personnel assigned to the agency on a strict need-to-know basis.
- You need not limit assignments until those on the access list actually see ULS or LAS information.
- Access-granting officials must control access to ULS and LAS reports for all supporting contractors.
- They must obtain approval from HQ AFSA/SEN, or their agency's access-granting official, before allowing personnel from other agencies to see ULS reports or briefings.

17. Access Record:

17.1. Attachments. The access-granting official must attach AF Form 481, **Access Record for Unauthorized Launch Study**, to each ULS report or briefing.

- For Secret and Confidential documents, permanently attach AF Form 481 to the front of the document with appropriate classification markings.
- For Top Secret reports, permanently attach AF Form 481 to the front of the document directly behind the AF Form 144, *Top Secret Access Record and Cover Sheet*.
- Each time individuals access a ULS document, they must enter their name, grade, social security number (SSN), organization, date of access, and signature on AF Form 481.
- If an individual needs daily access, a monthly annotation is sufficient.
- The access-granting official can allow administrative access to a ULS for auditing reports. Auditing access does not require annotation on AF Form 481 if access only discloses the name and document number of the ULS.
- At the end of each calendar year, the access-granting official must send HQ AFSA/SEN a copy of all AF Forms 481 with new entries.

17.2. Controlling Access to Briefings. Any agency that presents or controls ULS briefings must control access to the briefings, according to paragraph **13.**

- They must inform individuals of assignment limitations before the briefing starts.
- The access-granting official asks each person attending the briefing to complete all entries on AF Form 481, and attaches the completed AF Form 481 to a copy of the briefing.
- The access-granting official keeps a copy of the briefing for a permanent record of access, and notifies, in writing, each affected individual (as outlined in paragraph **19.** and **Attachment 1**) immediately after the briefing.

Section F—Assignment Limitations

18. Extent of Limitations:

18.1. Assignment Limitations. Assignment limitations apply to all military and civilian personnel identified on a ULS access record (either an AF Form 481, or a previous list) who prepared, or accessed, the contents of a ULS report, or who accessed ULS data before joining the Air Force. To limit assignments:

- Enter assignment limitation codes or statements in the personnel records of each Air Force military or civilian employee, according to paragraph **19.2.**
- Do not give civilian contractors a limitation code, since they do not have designated positions Keep a permanent record of their access in case they join the military or civilian government.
- Prohibit anyone who accessed a ULS or an LAS from being part of a Two-Person Concept team that handles, or has access to, the component or system covered by the ULS or LAS.
- Direct all questions on the applicability of assignment limitations to HQ AFSA/SEN.

18.2. Permanency of Limitations. Assignment limitations are permanent. In the event of a major weapon system modification, an individual can forward a waiver request to HQ AFSA/SEN through command channels.

18.3. Non-Precluding. A person carrying assignment limitation can nonetheless perform supervisory duties over individuals in the identified positions if those duties do not include participating as a Two-Person Concept team member.

19. Notification Responsibilities:

19.1. Responsibilities of Access-Granting Officials:

- Notify individuals of the assignment limitations before they access ULS reports, briefings, or data. Individuals can choose to decline access, without prejudice, if they want certain duties that would otherwise be denied. Access is granted and limitations imposed when the individual accepts.
- Notify individuals and their personnel office in writing (see **Attachment 1** for sample letter) of assignment limitations for each weapon system as soon as possible after they get initial access to ULS information. When you are not sure whether or not an individual has an assignment limitation on file, contact the servicing personnel office or HQ AFSA/SEN. The notification letter:
- Gives the individual's name, grade, and SSN.
- Refers to this instruction as authority for the assignment limitation.
- Specifies the weapon system for which access was granted.
- Send the notification letter to the individual and the personnel office that controls the personnel records, with a copy to HQ AFSA/SEN. Ask the affected personnel office to permanently file a copy of the letter in the individual's personnel records, as specified in paragraph **19.2.**

19.2. Recording Assignment Limitations. Record assignment limitations in personnel records.

19.2.1. The military personnel flight (MPF) updates the automated personnel data system with assignment limitation code M, according to AFI 36-2112, *Assignments* (formerly AFR 36-20), and files the letter in the unit personnel record group.

19.2.2. The central civilian personnel office (CCPO) files a copy of the letter of notification in the individual's official personnel folder. The supervisor enters the following notation on the AF Form 971, **Supervisor's Employee Brief**: "Assignment restrictions are imposed under AFI 91-106."

19.3. Form Prescribed. AF form 481.

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

Attachment 1

GLOSSARY OF ABBREVIATIONS AND ACRONYMS

Abbreviations and Acronyms

AFSA—Air Force Safety Agency

AFSA/SEN—AFSA, Directorate of Nuclear Surety

AFSA/SENA—AFSA/SEN, Nuclear Systems Engineering Division

CCPO—Central Civilian Personnel Office

CDR—Critical Design Review

CWI—Completion Without Intervention

DoD—Department of Defense

FSD—Full-Scale Development

HQ AFSA—Headquarters, AFSA

LAP—Launch Activation Path

LAS—Launch Action Study

MAJCOM—Major Command

MPF—Military Personnel Flight

NWSSG—Nuclear Weapon System Safety Group

SSN—Social Security (Account) Number

TF—Technical Feasibility

TNSA—Technical Nuclear Safety Analysis

UL—Unauthorized Launch

ULS—UnauthorizedLaunch Study

Attachment 2

SAMPLE NOTIFICATION LETTER

FROM: Access-granting official

SUBJ: Notification of Assignment Limitation

TO: Individual's name, grade, and SSN MPF or CCPO (Records Section)

1. **For the individual:** This assignment will limit your future assignments to (specify weapon system according to paragraph **18.1.**) units outlined in AFI 91-106. This assignment limitation results from your access to (specify report for which access was documented). The imposed restriction is permanent. In the event of a major weapon system modification, you can request a waiver from HQ AFSA/SEN, 9700 Avenue G, Kirtland AFB NM 87117-5671, through command channels.
2. **For MPF or CCPO**: File a copy of this letter in the individual's personnel folder. (***Note: For military personnel, refer to paragraph* 19.** 2.1 of this instruction; for civilian personnel, refer to paragraph **19.2.2.**)

(Signature and title of access-granting official)

cc: Individual's Supervisor (Civilian Only)
HQ AFSA/SENA