



Chapter 7

Nuclear Surety

7.1 Overview

A primary responsibility of the Department of Defense and Department of Energy stockpile mission is to ensure U.S. nuclear weapons are safe, secure, reliable, and under positive control, a concept commonly referred to as “surety.” This chapter provides a basic understanding of the various elements contributing to nuclear weapons surety.

7.2 Dual-Agency Surety Responsibilities

The DoD and the DOE, working through the National Nuclear Security Administration, share primary responsibility for the safety, security, and control of U.S. nuclear weapons. A 1983 DoD-DOE Memorandum of Understanding (MOU), signed by the Secretaries of Defense and Energy, reaffirmed “the obligation of the DoD and the DOE to protect public health and safety provides the basic premise for dual-agency judgment and responsibility for safety, security, and control of nuclear weapons.” In 2011, Deputy Secretaries of Defense and Energy signed a DoD-DOE *Nuclear Physical Security Collaboration*

Memorandum, which further solidified DoD-DOE commitment to develop common standards for the physical security of nuclear weapons and special nuclear material (SNM).

Because a nuclear weapon is in DoD custody for the majority of its lifetime, the DoD is responsible for a wide range of operational requirements, including accident prevention and response. The DOE/NNSA is responsible for the design, production, assembly, surety technology, disassembly, and dismantlement of U.S. nuclear weapons. The DOE/NNSA is also responsible for the transportation of weapons to and from the Military First Destination (MFD). There are, however, overlaps in responsibility between the DoD and the DOE/NNSA, requiring considerable coordination between the two regarding surety issues. For example, the DoD and the DOE/NNSA share responsibility for the interface between the weapon and the delivery system.

Because a nuclear weapon is in DoD custody for the majority of its lifetime, the Department of Defense is responsible for a wide range of operational requirements, including accident prevention and response.

7.3 National Policy

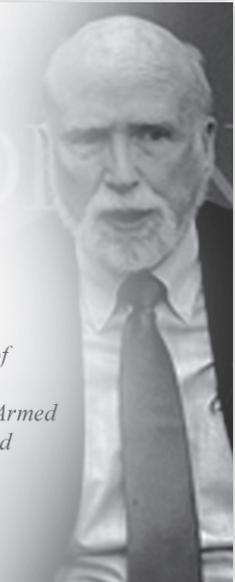
National policy provides guidance for coordinated interagency efforts concerning safety, security, and control across the nuclear enterprise. National Security Presidential Directive (NSPD) 28, *U.S. Nuclear Weapons Command and Control, Safety, and Security*, was issued on June 20, 2003. The document supersedes three former presidential directives:

- National Security Decision Memorandum 312, *Nuclear Weapons Recovery Policy* (1975);
- National Security Decision Directive 281, *Nuclear Weapons Command and Control* (1987); and
- National Security Decision Directive 309, *Nuclear Weapons Safety, Security, and Control* (1988).

NSPD-28 provides explicit guidance and standards in three nuclear weapons-related areas: nuclear command, control, and communications (NC3); nuclear weapons safety; and nuclear weapons security. Ongoing interagency-coordinated revisions for the presidential guidance accounts for these areas and reaffirms the necessity of continued diligence throughout the nuclear enterprise.

7.4 Nuclear Weapon System Safety

Nuclear weapons systems require special safety considerations due to the weapons' unique destructive power and the catastrophic consequences of an accident or unauthorized act. Nuclear weapons system safety refers to the collection of positive measures designed to minimize the possibility of a nuclear detonation resulting from accidents, unauthorized actions, inadvertent errors, or acts of nature. For safety purposes, a nuclear detonation is defined as an instantaneous release of energy from nuclear events (i.e., fission or fusion) exceeding the energy released from an explosion of four pounds of TNT. Nuclear safety also encompasses design features and actions to reduce the potential for dispersal of radioactive materials in the event of an accident. Nuclear weapons system safety integrates policy, organizational responsibilities, and the conduct of safety-related activities throughout the life-cycle of a nuclear weapon system. For additional information see DoD Directive (DoDD) 3150.08, *DoD Response to Nuclear and Radiological Incidents*.



“We place high priority on maintaining and improving safety and security. Our nuclear safety record is extraordinary.”

*Edward L. Warner, III,
Former Assistant Secretary of
Defense for Strategy and
Threat Reduction, Senate Armed
Services Committee Prepared
Remarks, March 31, 1998*

The nuclear weapon safety philosophy deviates from many other performance criteria, insofar as safety is not synonymous with reliability. Safety is concerned with how things fail, as opposed to focusing on what must work for reliability, and relies mostly on passive approaches rather than on active ones. For instance, an airplane is considered safe as long as critical systems, such as the engines and landing gear, work reliably. Active intervention (i.e., the pilot) is relied upon for accident prevention. With nuclear weapons, however, safety requirements must be met in the event of an accident, with or without human intervention. For nuclear weapons, reliability is the probability that a weapon will perform in accordance with its design intent or requirements, whereas safety focuses on preventing a nuclear detonation under all circumstances, except when directed by the President. High reliability is required for expected operational, or normal,

wartime employment environments. Safety is required for normal wartime employment environments, normal environments, and abnormal environments.

7.4.1 DoD and DOE Surety Programs

The objective of the DoD Nuclear Weapons Surety Program and the DOE Nuclear Explosive and Weapon Surety Program is to ensure adequate security of nuclear weapons and to prevent the inadvertent or unauthorized use of U.S. nuclear weapons. DoD Surety Standards are promulgated under DoDD 3150.02, *DoD Nuclear Weapons Surety Program*. The DOE continues to revise its standards to emphasize its responsibilities for nuclear explosive operations with DOE Order (DOE O) 452.1E, *Nuclear Explosive and Weapon Surety Program*. Although the operating environments differ significantly, DoD and DOE standards share many similarities. **Figure 7.1** compares DoD and DOE nuclear weapons surety standards.

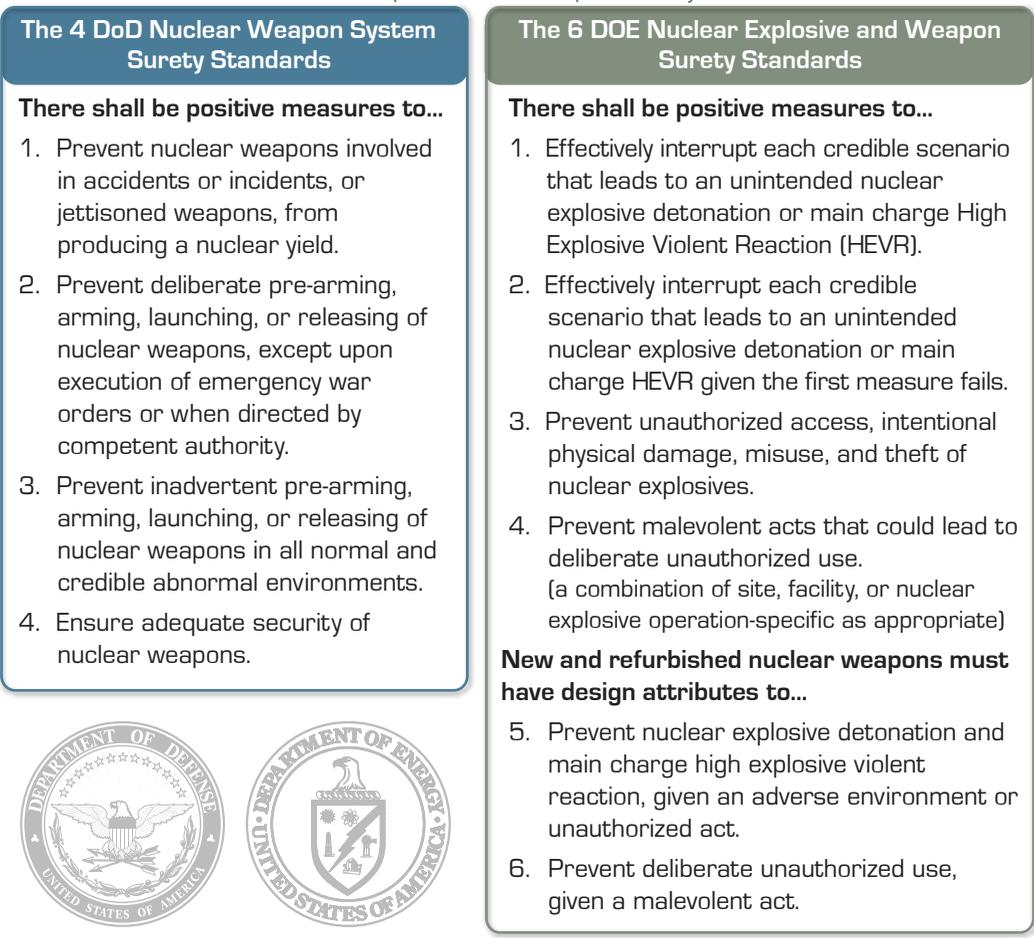
7.4.2 Nuclear Weapon Design Safety

Modern nuclear weapons incorporate a number of safety design features. These features provide high assurance that an accident, or other abnormal environment, will not produce a nuclear detonation. These also minimize the probability that an accident or other abnormal environment will cause the scattering of radioactive material. In the past, there have been performance trade-offs to consider in determining whether to include various safety features in the design of a particular warhead. Thus, not all warhead-types incorporate every available safety feature. However, all legacy warheads were designed to meet specific safety criteria across the range of both normal and abnormal environments.

Normal environments are the expected logistical and operational environments, as defined in a weapon's military characteristics (MCs) and stockpile-to-target sequence (STS) documents, in which the weapon is expected to survive without degradation in operational reliability. Normal environments include a spectrum of conditions that the weapon could be subjected to in anticipated peacetime logistical situations and in wartime employment conditions up to the moment of detonation. For example, a normal environment may include conditions such as a temperature range of minus 180 to plus 155 degrees Fahrenheit, a force of 10G set-back upon missile launch, or shock from an impact of a container being dropped from a height of up to two inches.

Abnormal environments are the expected logistical and operational environments, as defined in a weapon's MCs and STS documents, in which the weapon is not expected to

Figure 7.1 Comparison of DoD Nuclear Weapon System Surety and DOE Nuclear Explosive and Weapon Surety Standards



retain full operational reliability. Abnormal environments include conditions not expected in normal logistical or operational situations but could occur in credible accidental or unusual situations, including an aircraft accident, lightning strike, shipboard fire, or a bullet, missile, or fragmentation strike.

The following are safety criteria design requirements for all U.S. nuclear weapons:

- *Normal environment*—Prior to receipt of the enabling input signals and the arming signal, the probability of a premature nuclear detonation must not exceed one in a billion per nuclear weapon lifetime.

- *Abnormal environment*—Prior to receipt of the enabling input signals, the probability of a premature nuclear detonation must not exceed one in a million per credible nuclear weapon accident or exposure to abnormal environments.
- *One-point safety*—The probability of achieving a nuclear yield greater than four pounds of TNT equivalent, in the event of a one-point initiation of the weapon’s high explosive, must not exceed one in a million.

Enhanced Nuclear Detonation Safety

Nuclear detonation safety deals with preventing nuclear detonation through accidental or inadvertent causes. For all current weapons in the U.S. stockpile, the firing system forms a key part of detonation safety implementation. The goal of nuclear safety design is to prevent inadvertent nuclear yield by isolating the components essential to weapon detonation from significant electrical energy. This involves the enclosure of detonation-critical components in a barrier to prevent unintended energy sources from powering or operating the weapon’s functions. When a barrier is used, a gateway is required to allow the proper signals to reach the firing set. A gateway can also be used to prevent the firing set stimulus from reaching the detonators. These gateways are known as *stronglinks*. The enhanced nuclear detonation safety (ENDS) concept is focused on a special region of the weapon system containing safety-critical components designed to respond to abnormal environments in a predictably safe manner. This ensures nuclear safety is achieved in an abnormal environment despite the appearance of premature signals at the input of the special region. **Figure 7.2** illustrates this modern nuclear safety architecture.

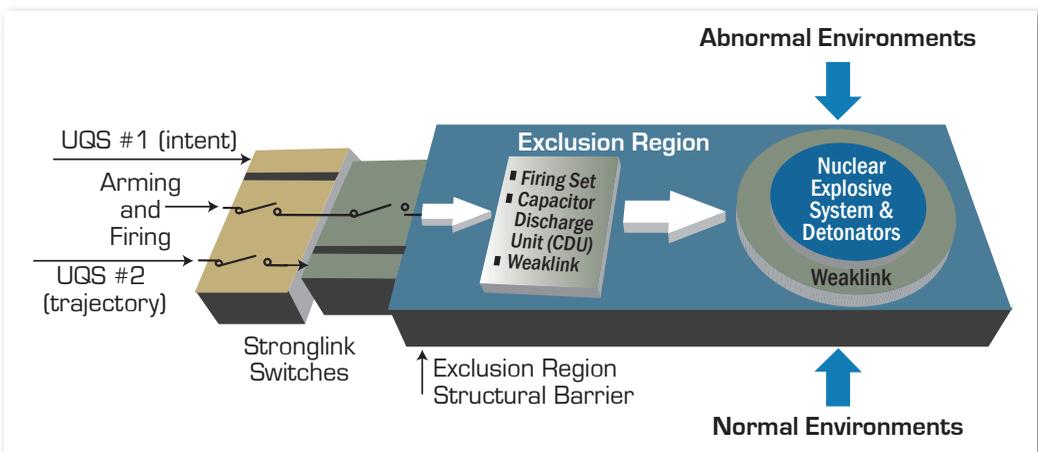


Figure 7.2 Modern Nuclear Safety Architecture

Stronglinks operate upon receipt of a unique signal (UQS). Stronglinks open only upon receipt of a unique signal indicating proper human intent (UQS #1) or a specific weapon trajectory (UQS #2). Stronglinks are designed to withstand severe accident environments including physical shock, high temperatures, and high voltage. Before stronglink failure occurs, another component is designed to render the firing set safe: the *weaklink*. The weaklink is designed so that, in the event that a certain part is ruptured, it will keep the weapon's electrical system in a safe mode, thereby preventing a nuclear detonation. Any force strong enough to pass the stronglink will rupture the weaklink, "freezing" the electrical system in a safe condition.

Modern safety requirements dictate that each firing set contains two independent stronglinks. The UQS for the intent stronglink cannot be stored in the weapon and must be entered by a human being. The unique signal pattern for the trajectory stronglink is frequently stored in a device known as a trajectory-sensing signal generator (TSSG).

The four principal safety themes for nuclear weapons are isolation, incompatibility, inoperability, and independence. The stronglink plays an important role in all four themes.

Isolation

The critical components necessary for a nuclear detonation are isolated from their surroundings by placing them within a physical barrier known as an exclusion region. This barrier blocks all forms of significant electrical energy, such as lightning or power surges, even when the exclusion region is subjected to a variety of abnormal environments.

The barrier is not perfect, only a perfect barrier would make a weapon perfectly safe. However, the result of perfect isolation is a non-functional weapon. To initiate a nuclear detonation, some energy must be permitted inside the exclusion region. Therefore, an energy gateway, or shutter, is required to complete the electrical circuit. When the shutter is closed, it should form an integral part of the barrier. When the shutter is opened, it should readily transfer energy inside the exclusion region to cause a nuclear detonation. Stronglinks are these energy gateways.

Incompatibility

It is critical to ensure only a deliberate act activates the stronglinks and opens the energy circuit. The act can originate from human intent or the delivery environments of the weapon. The stronglink serves as an electrical combination lock preventing weapon usage until deliberate action occurs. The combination to the lock is a complex pattern

of binary pulses. To activate the stronglink switch, an operator must input the unique signal information when the weapon is ready for use. This information is converted into a unique pattern of long and short electrical pulses, which is the only signal that will activate the stronglink and any other pattern is incompatible. An incompatible pattern will cause the switch to lock up and remain in a safe condition. **Figure 7.3** illustrates the concept of incompatibility.

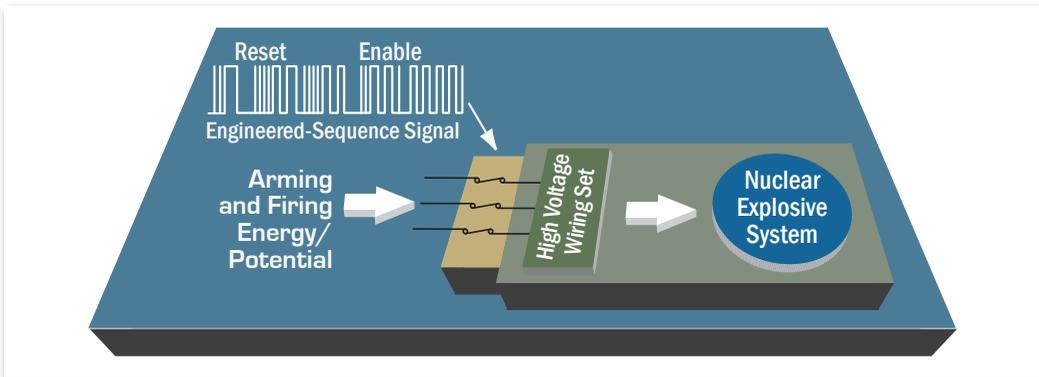


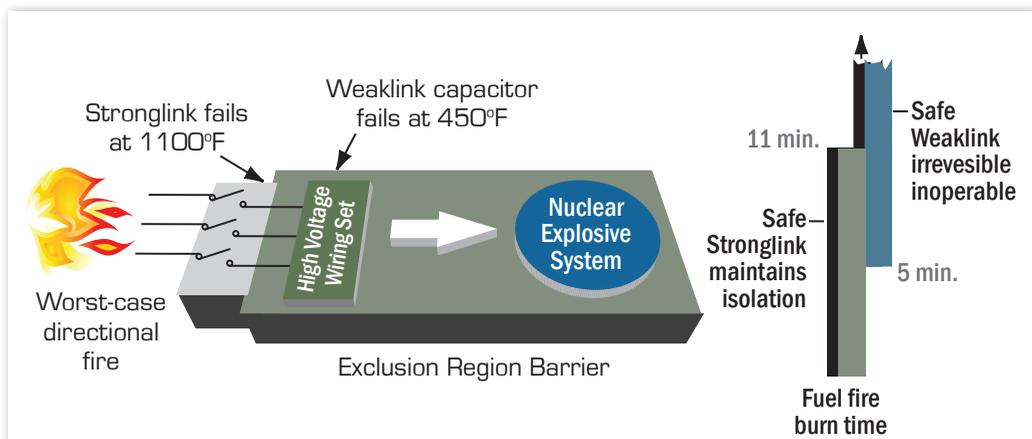
Figure 7.3 Incompatibility

Each stronglink contains one pattern and can only be operated by receiving its unique pattern. Stronglink patterns are analyzed for their uniqueness to ensure they are incompatible with naturally occurring signals. Additionally, stronglinks are engineered so that the probability of their accidental activation from a naturally occurring source is far less than one in a million.

Inoperability

At some level of exposure to an abnormal environment, the energy from the surroundings becomes so intense the barrier loses its integrity and melts or ruptures. Incorporating environmental vulnerability into weaklinks ensures nuclear safety. Weaklinks perform the opposite function of stronglinks. They must be functional for a nuclear detonation, but weaklinks are designed to fail at relatively low environmental levels, thus rendering the weapon inoperable. These levels are low enough to ensure the weaklink fails before the stronglink or exclusion barrier fails. At the same time, weaklinks are designed to withstand the normal activity experienced during the storage and shipping throughout the stockpile-to-target sequence. Ideally, the weaklinks are co-located with the stronglink so both components experience the same environmental assault. **Figure 7.4** is a diagram of the concept of inoperability.

Figure 7.4 Inoperability



Independence

Typically, two different stronglinks with different patterns are used in each weapon to provide the required assurance of safety. With independent stronglinks, a flaw may cause one stronglink to fail, but the other stronglink will still protect the weapon.

Insensitive High Explosive

An intrinsic feature of nuclear weapon design safety is the use of insensitive high explosive (IHE), as opposed to conventional high explosive. By reducing sensitivity to shock or heat, a weapon is more resistant to accidental detonation and represents a great advance in safety by reducing the likelihood of plutonium scatter.

Fire-Resistant Pit

Another feature of nuclear weapons design safety is the fire-resistant pit (FRP). In an accident, plutonium can be dispersed if it is aerosolized by intense heat, such as that from ignited jet fuel. To prevent this, the nuclear weapon pit can be designed with a continuous barrier around it. In theory, this barrier will contain the highly corrosive, molten plutonium for a sufficient amount of time to extinguish the fire.

7.5 Nuclear Weapons Security

Nuclear weapons security refers to the range of active and passive measures employed to protect a weapon from access by unauthorized personnel and to prevent loss or damage. These measures include nuclear security policy; security forces; equipment; technology;



tactics, techniques, and procedures (TTPs); and personnel security standards. Ensuring security is vital throughout the entire life-cycle of a weapon, as it contributes directly to the shared surety objectives of both DoD and DOE/NNSA.

The Departments of Defense and Energy are responsible for providing appropriate security for all nuclear weapons in their custody. Custody is defined as the responsibility for controlling the transfer, movement, and access to a nuclear weapon or its components. Inherent in these custodial responsibilities is control and the custodial agent must secure the weapon to ensure positive control is maintained at all times. If unauthorized access is obtained by an adversary, the control is lost but custody is maintained.

7.5.1 DoD Nuclear Weapon Security Standard

DoDD 5210.41, *Security Policy for Protecting Nuclear Weapons*, establishes the DoD Nuclear Weapon Security Standard (NWSS). The objectives of the standard include:

- prevent unauthorized access to nuclear weapons;
- prevent loss of control; and
- prevent, to the maximum extent possible, radiological contamination caused by unauthorized acts.

The NWSS defines two fundamental tenets of nuclear weapons physical security. The first tenet is “to deny unauthorized access to nuclear weapons,” and the second is “failing denial of unauthorized access, commanders will take any and all actions necessary...to immediately reestablish security, prevent loss, or regain control of nuclear weapons.”

The overriding objective of nuclear weapons security is *denial* of unauthorized access. This is achieved by employing physical features, technical devices, or security measures and forces in an integrated, defense-in-depth concept that leverages five distinct security capabilities. Together, the security capabilities support the NWSS and are commonly referred to as the five “Ds” of nuclear security, deter, detect, delay, deny, and defeat (**Figure 7.5**).

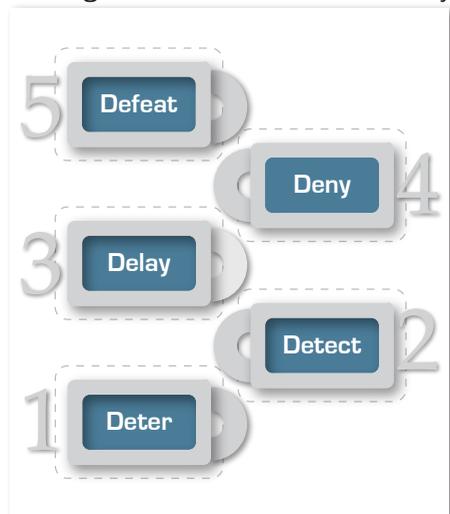


Figure 7.5 The 5 “Ds” of Nuclear Security

First, a security system must be sufficiently robust to *deter* adversaries from attempting to achieve unauthorized access. Deterrence is accomplished through facility hardening; security forces tactics, techniques, and procedures; and an aggressive counterintelligence program.

If deterrence fails, a security system must ensure rapid *detection* of an adversary's presence and intention as far away from the nuclear weapon as practical. Detection is achieved through close coordination between law enforcement and the intelligence community coupled with an integrated system of alarms, sensors, procedural requirements, and human surveillance (e.g., patrols).

In concert with detection, security systems must sufficiently *delay* adversaries from gaining unauthorized access before armed security forces can respond. Delay is achieved through physical security barriers, facility hardening, response forces, and the design features of the weapons storage facility.

Security forces must *deny* adversaries unauthorized access to nuclear weapons. Denial is achieved through lethal or non-lethal technological means, or by creating adversarial duress sufficient to prevent unauthorized access.

If denial fails, however, security forces and systems must *defeat* a hostile adversary and immediately regain control of the nuclear weapon.

The DoD Mighty Guardian (MG) program is designed to ensure vulnerabilities are identified and potential risks are minimized. The MG process combines force-on-force exercises and engineering assessments to evaluate the effectiveness of nuclear security policy and standards. MG results are used to improve the U.S. nuclear security system. Commanders use risk management principles to identify potential risks to nuclear weapons and to prioritize risk reduction requirements. The DoD Nuclear Security Risk Management Model assists commanders in this responsibility and incorporates security enhancements into the *DoD Nuclear Weapons Physical Security (NWPS) Roadmap*. The Roadmap examines the current state of NWPS and plans for the future to ensure security capabilities are adequate to meet the NWSS.

To develop a standardized approach to nuclear security, as it is applied to DoD-DOE nuclear weapons environments, the 2011 DoD-DOE *Nuclear Physical Security Collaboration Memorandum* pledges to develop and use a common threat assessment, the Nuclear Security Threat Capabilities Assessment (NSTCA), and methodology to identify and assess

threat capabilities and determine nuclear weapons security vulnerabilities. The NSTCA is developed, reviewed annually, and updated as necessary to support the preparation of unit or facility vulnerability assessments.

7.5.2 DOE Safeguards and Security

The DOE/NNSA has programs similar to those of the DoD to ensure the physical security of nuclear weapons and SNM in transport to and from DOE/NNSA locations, national laboratories, and plants. Like the DoD, the DOE/NNSA evaluates its future security capabilities to ensure adequate security is provided to meet identified threats.

7.5.3 DoD and DOE Personnel Security

Both the DoD and the DOE have personnel reliability assurance programs to ensure personnel assigned to nuclear weapons-related duties are trustworthy. The DoD Personnel Reliability Program (PRP) and the DOE Human Reliability Program (HRP) ensure trustworthy personnel possess the necessary judgment to work with nuclear weapons. Unescorted access to nuclear weapons is limited to those who are subject to a DoD or DOE personnel reliability program.

The DoD-PRP is designed to ensure the highest possible standards of individual reliability for those personnel assigned to nuclear weapons duties. It emphasizes the importance of the individual's loyalty, integrity, trustworthiness, behavior, and competence. The program applies to all personnel who handle nuclear weapons, nuclear weapon systems, or nuclear components as well as to those who have access to nuclear weapons. DoD and DOE personnel reliability programs ensure authorized access to nuclear weapons is limited to those personnel who have been carefully screened and certified.

Before personnel are assigned to designated DoD-PRP or DOE-HRP positions, a screening process is conducted that includes a:

- personal security investigation and the granting of a security clearance;
- medical evaluation or screening to determine the physical fitness of the individual;
- review of relevant quality indicators through a check of the individual's personnel file and any other locally available, and relevant, information;
- verification of professional qualifications to ensure the individual is qualified to perform the duties required of the position assigned; and

- personal interview to stress the importance of the duties assigned and provide opportunity for the individual to disclose information that may affect the final decision to certify under the applicable reliability program.

The most important aspect of procedural security is the two-person rule, which requires the presence of at least two cleared, PRP- or HRP-certified, and task-knowledgeable individuals whenever there is authorized access to a nuclear weapon.

The certifying official is responsible for determining a person's overall reliability and for assigning the individual to a substantive nuclear weapons-related position.

Once a person begins to perform duties in a DoD-PRP or DOE-HRP position, the individual is periodically evaluated to ensure continued conformity to reliability standards. Any information raising questions or concerns about an individual's judgment or reliability is subject to review. Personnel who cannot meet the standards are disqualified from the program and relieved of their nuclear weapons-related responsibilities.

7.5.4 Procedural Security

The most important aspect of procedural security is the *two-person rule*, which requires the presence of at least two cleared PRP- or HRP-certified, task-knowledgeable individuals whenever there is authorized access to a nuclear weapon. Each person is required to be capable of detecting incorrect or unauthorized actions pertaining to the task being performed. Restricted entry to certain sectors

and exclusion areas based on strict need-to-know criteria reduces the possibility of unauthorized access.

7.5.5 DoD and DOE Security Program Authorities

Within the United States, nuclear weapon security programs are governed by DoD and DOE policy. For U.S. nuclear weapons in other countries, the United States has established Programs of Cooperation to delineate the duties and responsibilities involved in the weapons' deployment. DoD policies and procedures for nuclear weapons security are found in DoDDs, DoD Instructions (DoDI), and DoD Manuals (DoDM). DOE/NNSA policies and procedures for nuclear weapons security and security of SNM are found in DOE Os and Defense Nuclear Security (DNS) implementing guidance.

DOD SECURITY PROGRAM AUTHORITIES

DoDD 5210.41, Security Policy for Protecting Nuclear Weapons, outlines the DoD security policy for protecting nuclear weapons in peacetime environments. It gives guidance to commanders to provide security for and to ensure the survivability of nuclear weapons. The directive also authorizes the publication of DoD S-5210.41-M, which is the DoD manual providing security criteria and standards for protecting nuclear weapons.

DoDI 5210.42, Nuclear Weapons Personnel Reliability Program, outlines DoD policy and assigns responsibility for the management of the DoD Nuclear Weapons PRP. This instruction also authorizes the publication of DoD Manual 5210.42-R that prescribes mandatory procedures for the DoD Nuclear Weapons PRP to ensure the safety and security of the U.S. nuclear deterrent mission.

DoDI O-5210.63, DoD Procedures for Security of Nuclear Reactors and Special Nuclear Materials, directs policy, responsibilities, procedures, and minimum standards for safeguarding DoD nuclear reactors and special nuclear material.

DoD S-5210.92-M, Physical Security Requirements for Nuclear Command and Control (NC2) Facilities, implements policy governing physical security requirements of U.S. NC2 facilities and systems that have the capability to make and transmit a nuclear control order as part of the NCCS.

DoDI 3224.03, Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E), provides guidance for the acquisition of all physical security equipment. It assigns responsibility for physical security equipment research, engineering, procurement, installation, and maintenance.

DOE SECURITY PROGRAM AUTHORITIES

DOE O 452.1E, Nuclear Explosive and Weapon Surety Program, outlines the Nuclear Explosive and Weapon Surety (NEWS) Program and the five DOE surety standards.

DOE O 452.2E, Nuclear Explosive Safety, addresses security regarding the safety of NNSA nuclear explosive operations.

DOE Policy 470.1A, Safeguards and Security Program, outlines the DOE Safeguards and Security Program, which provides the basis for security for all DOE/NNSA activities related to nuclear weapons. 10 CFR Part 712, Human Reliability Program, establishes the policies and procedures for implementation of the HRP within the DOE, including the NNSA. This document consolidates and supersedes two former programs, the Personnel Assurance Program and the Personnel Security Assurance Program.

DOE O 470.3B, Graded Security Protection (GSP) Policy, establishes the design basis threat which facilities that possess nuclear weapons must protect against.

DOE O 472.2 Chg 2, Personnel Security, establishes requirements that enables DOE to operate a successful, efficient, cost-effective personnel security program to ensure accurate, timely, and equitable determinations of individuals' eligibility for access to classified information and SNM, including nuclear weapons.

DOE O 474.2 Admin Chg 3, Nuclear Material Control and Accountability, establishes performance objectives, metrics, and requirements for developing, implementing, and maintaining a nuclear material control and accountability program, including nuclear weapons, within DOE/NNSA.

DOE O 473.3, Protection Program Operations, establishes requirements for the management and operation of the DOE Federal Protective Forces (FPF), Contractor Protective Forces (CPF), and the Physical Security of property and personnel under the cognizance of DOE, including those which protect nuclear weapons.



7.6 Use Control

The term use control refers to the collection of measures that facilitate authorized use of nuclear weapons but protect against deliberate unauthorized use. These measures include a combination of weapon design features and operational procedures.

Use control is achieved by designing weapon systems with electronic and mechanical features that prevent unauthorized use and allow authorized use. Not all use control features are installed on every weapon system.

Weapons System Coded Control

Both strategic nuclear missile systems and strategic heavy bomber aircraft use system coded control. Intercontinental ballistic missile (ICBM) crews require an externally transmitted launch code in order to dispatch a missile. Similarly, ballistic missile submarine (SSBN) crews require an externally transmitted authorization code to launch a submarine-launched ballistic missile (SLBM). Strategic bomber crews use a pre-arming circuit that also requires an externally transmitted authorization code to employ nuclear bombs or cruise missiles. The externally transmitted authorization code is received via nuclear control order or emergency action message (EAM).

Coded Control Device

A coded control device (CCD) is a use control component that may be a part of the overall weapons system coded control.

Command Disablement System

The command disablement system (CDS) allows for manual activation of the non-violent disablement of essential weapons components, which renders the warhead inoperable. The CDS may be internal or external to the weapon and requires human initiation. The CDS is not installed on all weapon systems.

Active Protection System

The active protection system (APS) senses attempts to gain unauthorized access to weapon-critical components. In response to unauthorized access, critical components are physically damaged or destroyed automatically. This system requires no human intervention for activation and is not installed on all weapons systems.

Environmental Sensing Device

The environmental sensing device (ESD) is a feature placed in the arming circuit of a weapon providing both safety and control. It prevents inadvertent functioning of the circuit

until the weapon is launched or released and experiences environmental parameters specific to its particular delivery system. For example, accelerometers are a common tool employed for this purpose.

Permissive Action Link

A permissive action link (PAL) is a device included in or attached to a nuclear weapon system in order to preclude arming and/or launching until the insertion of a prescribed,



Figure 7.6 Entering PAL Authorization Code

discrete code or combination. It may include equipment and cabling external to the weapon or weapon system to activate components within the weapon or weapon system. Most modern U.S. PAL systems include a multiple-code coded switch (MCCS) component. **Figure 7.6** shows an individual entering a PAL authorization code into a bomb during an exercise.

7.6.1 DoD Use Control Program

The DoD has broad responsibilities in the area of nuclear weapons use control. DoDI S-3150.07, *Controlling the Use of Nuclear Weapons*, establishes policies and responsibilities for controlling the use of nuclear weapons and nuclear weapons systems. It describes:

- the President as the sole authority for employing U.S. nuclear weapons;
- a layered approach to protecting weapons;
- positive measures to prevent unauthorized access and use;
- methods to counter threats and vulnerabilities; and
- the legal and policy requirements to ensure presidential control while simultaneously facilitating authorized use in a timely manner.

7.6.2 DOE/NNSA Use Control Program

Use control responsibilities of the DOE/NNSA include the design and testing of new use control features and their installation into the nuclear weapon. Additionally, the national laboratories provide technical support to reinforce DoD use control efforts. The DOE/NNSA Nuclear Explosive and Weapon Security and Control Program comprises an integrated system of devices, design techniques, and other methods to maintain control of nuclear explosives and nuclear weapons at all times. These use control measures allow use, when authorized and directed by proper authority, and protect against deliberate unauthorized use (DUU). Major elements of the program include:

- use control measures for nuclear explosives and weapons, including design features incorporated and used at the earliest practical point during assembly and removed at the latest practical point during disassembly or dismantlement; and
- measures to assist in the recapture or recovery of lost or stolen nuclear explosives or nuclear weapons.

The DOE/NNSA program encompasses the development, implementation, and maintenance of standards, plans, procedures, and other measures. These include the production of equipment designed to ensure the safety, security, and reliability of nuclear weapons and components in coordination with the DoD. The DOE/NNSA conducts research and development on a broad range of use control methods and devices for nuclear weapons and assists the DoD in developing, implementing, and maintaining plans, procedures, and capabilities to store and move nuclear weapons. The DOE/NNSA also assists other departments in developing, implementing, and maintaining plans, procedures, and capabilities to recover lost, missing, or stolen nuclear weapons or components.

