U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-2203

Glossary of Security Terms for Nuclear Power Reactors

Office of Nuclear Security and Incident Response

AVAILABILITY OF REFERENCE MATERIALS IN NRC PUBLICATIONS

NRC Reference Material

As of November 1999, you may electronically access NUREG-series publications and other NRC records at NRC's Library at www.nrc.gov/reading-rm.html. Publicly released records include, to name a few, NUREG-series publications; *Federal Register* notices; applicant, licensee, and vendor documents and correspondence; NRC correspondence and internal memoranda; bulletins and information notices; inspection and investigative reports; licensee event reports; and Commission papers and their attachments.

NRC publications in the NUREG series, NRC regulations, and Title 10, "Energy," in the *Code of Federal Regulations* may also be purchased from one of these two sources.

1. **The Superintendent of Documents**
   U.S. Government Publishing Office
   Mail Stop IDCC
   Washington, DC 20402-0001
   Internet: bookstore.gpo.gov
   Telephone: (202) 512-1800
   Fax: (202) 512-2104

2. **The National Technical Information Service**
   5301 Shawnee Rd., Alexandria, VA 22312-0002
   www.ntis.gov
   1-800-553-6847 or, locally, (703) 605-6000

A single copy of each NRC draft report for comment is available free, to the extent of supply, upon written request as follows:

Address: **U.S. Nuclear Regulatory Commission**
Office of Administration
Publications Branch
Washington, DC 20555-0001
E-mail: distribution.resource@nrc.gov
Facsimile: (301) 415-2289

Some publications in the NUREG series that are posted at NRC's Web site address www.nrc.gov/reading-rm/doc-collections/nuregs are updated periodically and may differ from the last printed version. Although references to material found on a Web site bear the date the material was accessed, the material available on the date cited may subsequently be removed from the site.

Non-NRC Reference Material

Documents available from public and special technical libraries include all open literature items, such as books, journal articles, transactions, *Federal Register* notices, Federal and State legislation, and congressional reports. Such documents as theses, dissertations, foreign reports and translations, and non-NRC conference proceedings may be purchased from their sponsoring organization.

Copies of industry codes and standards used in a substantive manner in the NRC regulatory process are maintained at—

The NRC Technical Library
Two White Flint North
11545 Rockville Pike
Rockville, MD 20852-2738

These standards are available in the library for reference use by the public. Codes and standards are usually copyrighted and may be purchased from the originating organization or, if they are American National Standards, from—

American National Standards Institute
11 West 42nd Street
New York, NY 10036-8002
www.ansi.org
(212) 642-4900

Legally binding regulatory requirements are stated only in laws; NRC regulations; licenses, including technical specifications; or orders, not in NUREG-series publications. The views expressed in contractorprepared publications in this series are not necessarily those of the NRC.

The NUREG series comprises (1) technical and administrative reports and books prepared by the staff (NUREG–XXXX) or agency contractors (NUREG/CR–XXXX), (2) proceedings of conferences (NUREG/CP–XXXX), (3) reports resulting from international agreements (NUREG/IA–XXXX), (4) brochures (NUREG/BR–XXXX), and (5) compilations of legal decisions and orders of the Commission and Atomic and Safety Licensing Boards and of Directors' decisions under Section 2.206 of NRC's regulations (NUREG–0750).

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NUREG-2203

Glossary of Security Terms for Nuclear Power Reactors

Manuscript Completed: March 2015
Date Published: February 2017

Prepared by:
Amy Roundtree
Wayne Chalk

Kris Jamgochian, NRC Project Manager

Office of Nuclear Security and Incident Response

ABSTRACT

This is a glossary of security terms specifically for nuclear power reactors that are commonly used in the nuclear industry and regulatory community. These terms were compiled from U.S. Nuclear Regulatory Commission and nuclear industry sources. This is published to assist agency authors, readers, and stakeholders in understanding common terms used in security.

CONTENTS

ABSTRACT.....iii

1. GLOSSARY OF SECURITY TERMS.....1

2. REFERENCES.....31

1. GLOSSARY OF SECURITY TERMS

10 CFR: Title 10, "Energy," of the *Code of Federal Regulations*. (Regulatory Guide (RG) 5.66, "Access Authorization Program for Nuclear Power Plants")

Access Authorization Compensatory Measures (AA CM): Order issued by the U.S. Nuclear Regulatory Commission for Compensatory Measures Related to Access Authorization, dated January 7, 2003.

access-denied: the clearance condition where an individual is not considered trustworthy and reliable based upon the reviewing official's evaluation of potentially disqualifying information.

access control: the control of entry or use, to all or part, of any physical, functional, or logical component of a critical digital asset (CDA).

accessible: describes a structure, system, or component with which an adversary could make physical contact without the aid of scaffolding or a ladder.

achievable target element: target element that is within the capabilities included in the design-basis threat.

action: functional parts of a firearm that move together to place a cartridge in the chamber or otherwise ready a cartridge for firing.

active insider: a person who, while in an unescorted access status and within the protected area, takes direct action to assist a design-basis threat (DBT) (e.g., participates in planning, uses an authorized key card to open a controlled access door, creates an operational or security diversion, or impedes a response to the threat).

active vehicle barrier: an obstacle with a changeable configuration that has two positions: one position that denies passage of a vehicle and a second position that allows vehicle passage.

active violent insider: a person who, while in an unescorted access status and within the protected area, takes direct action to harm plant components, a member of the security force, or plant staff with the intent of preventing the operation of equipment or of preventing the person harmed from participating in protective or recovery strategies, or who takes action to engage and/or divert operations or security resources from normal protective or recovery strategies.

administrative withdrawal of UAA/UA: a process to temporarily withhold unescorted access authorization (UAA) or unescorted access (UA) from an individual while action is taken to complete or update an element of the UAA requirements.

adversary: an individual who has not been granted unescorted access to a site's protected area, or access to a site's critical systems, who attempts (or is actively engaged in

planning for or attempting) to gain unauthorized entry to the protected or vital areas, or access to a site's critical systems for the purposes of committing an act of radiological sabotage.

adverse impact: a direct deleterious effect on a critical digital asset (e.g., loss or impairment of function; reduction in reliability; reduction in ability to detect, delay, assess, or respond to malevolent activities; reduction of ability to call for or communicate with offsite assistance; or reduction in emergency response ability to implement appropriate protective measures in the event of a radiological emergency). Cases in which the direct or indirect compromise of a support system causes a safety, important-to-safety, or emergency-preparedness system or support system to actuate or "fail safe" and not result in radiological sabotage (i.e., causes the system to actuate properly in response to established parameters and thresholds) are not considered to be adverse impacts as defined in 10 CFR 73.54(a).

aircraft imminent threat: a threat that meets one of the following conditions: (1) a large-threat aircraft is heading toward and is within 5 minutes of a site, and an altitude change aligns a large-threat aircraft with a site; (2) a large-threat aircraft is locally observed; or (3) a site receives specific, credible intelligence that a small aircraft heading toward the site presents a greater threat than its size would indicate, and the estimated time to the site is 5 minutes or less.

aircraft informational threat: a threat that meets one of the following conditions: (1) a large-threat aircraft is heading toward but is more than 30 minutes from a site; or (2) the threat is a small aircraft and the site has either observed the threat aircraft locally or has not received specific, credible intelligence information that the aircraft presents a threat greater than its size would indicate.

aircraft probable threat: a threat that meets one of the following conditions: (1) a large-threat aircraft is heading toward and is greater than 5 but less than 30 minutes from a site, or (2) a site receives specific, credible intelligence that a small aircraft heading toward the site presents a greater threat than its size would indicate, and the estimated time to the site is greater than 5 but less than 30 minutes.

alarm station operator: a person responsible for, but not limited to, monitoring security systems, assessing alarms, initiating response to a security threat, and making notifications to both onsite and offsite support agencies in accordance with site procedures.

annual/annually: requirements specified as "annual" should be scheduled at a nominal 12 months. Performance may be conducted up to three months before to three months after the scheduled date. The next scheduled date is 12 months from the originally scheduled date, unless a mid-cycle activity is conducted to establish a new schedule date.

any failure, degradation, or discovered vulnerability: the performance of a security safeguards measure has been reduced to the degree that it is rendered ineffective for the intended purpose. This includes cessation of proper functioning or performance of equipment, personnel, or procedures that are part of the physical protection program

necessary to meet the requirements of 10 CFR Part 73, "Physical Protection of Plants and Materials," or a discovered defect in such equipment, personnel, or procedures that degrades their function or performance to a degree that could be exploited for the purpose of committing acts described in Appendix G, "Reportable Safeguards Events," to 10 CFR Part 73.

apparent-cause investigation: the use of abbreviated investigation techniques and readily available information to correct a specific problem. A formal root-cause analysis is not expected. An apparent-cause investigation should provide a reasonable degree of confidence that the implementation of the corrective action(s) for the apparent cause(s) will correct (not prevent the recurrence of) the problem. The last part of the investigation should address whether the significance level of the problem should be increased and additional investigation is needed. An apparent cause is most probable cause of the problem using abbreviated investigation technique.

applicant: applicants for an operating license or holders of a combined construction permit and operating license (combined license), who choose to implement their access authorization programs, which were approved by the Commission in their Physical Security Plan, prior to receiving their operating licenses or their Commission findings.

armed escort: an armed person, not necessarily uniformed, whose primary duty is to accompany shipments of special nuclear material for the protection of such shipments against theft or radiological sabotage.

armed responder: an armed member of the security organization who:

- is trained and qualified in accordance with the training and qualification plan.
- must be immediately available at all times inside the protected area to implement the protective strategy and is supported in this role by other onsite and offsite resources. "Immediately available" means having the ability to respond within the timelines required to effectively implement the site protective strategy.
- has the primary responsibility of responding to threats against the facility up to and including the DBT.
- may be assigned other duties that do not prevent them from effectively responding in accordance with the protective strategy. They are not assigned any duties that would impede an effective response.
- is equipped with or has readily available (if at a stationary post) a contingency weapon.
- has ready access to body armor, gas mask, and other equipment as appropriate to assure an effective response. "Ready access" means that the responder is able to pick up the equipment en route within required timelines.

armed response personnel: persons, not necessarily uniformed, whose primary duty in the event of attempted theft of special nuclear material or radiological sabotage shall be to respond, armed and equipped, to prevent or delay such actions.

armed security officer: an armed member of the security organization who:

- is trained and qualified to perform duties and responsibilities involving the possession and use of assigned firearms.
- may or may not be designated to respond to a contingency event.
- has ready access to a contingency weapon, body armor, gas masks, and other equipment as appropriate to respond in effectively implementing their role in the protective strategy.

attempts to cause: efforts to accomplish a threat, even though it has not occurred or has not been completed because it was interrupted, stopped before completion, or may occur in more than 2 hours, as established through reliable and substantive information.

automated: an assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Used in both the singular and plural cases.

automatic: a firearm using gas pressure or force of recoil and mechanical spring action for repeatedly performing the entire firing cycle (i.e., fire, unlock, extract, eject, cock, feed, chamber, and lock) with a single press of the trigger.

authentication: verifying the identity of a user and application acting as a user or verifying the origin of a data, messages, or commands. Authentication depends on four cases of data, generally summarized as “what you know,” “what you have,” “what you are,” and “what you do.”

authorized individual: any individual, including an employee, a student, a consultant, or an agent of a licensee who has been designated in writing by a licensee to have responsibility for surveillance of or control over special nuclear material or to have unescorted access to areas where special nuclear material is used or stored.

authorized personnel: those personnel granted unescorted access to the Protected Area and/or Vital Area(s), as well as those granted access with escort.

background check: includes, at a minimum, a Federal Bureau of Investigation (FBI) criminal history records check (including verification of identity based on fingerprinting), employment history, education, and personal references. Individuals engaged in activities subject to regulation by the Commission, applicants for licenses to engage in Commission-regulated activities, and individuals who have notified the Commission in writing of an intent to file an application for licensing, certification, permitting, or approval of a product or activity subject to regulation by the Commission are required under 10 CFR 73.57, “Requirements for Criminal History Records Checks of Individuals Granted Unescorted Access to a Nuclear Power Facility, a Non-Power Reactor, or

Access to Safeguards Information," to conduct fingerprinting and criminal history records checks before granting access to Safeguards Information. A background check must be sufficient to support the trustworthiness and reliability determination so that the person performing the check and the Commission has assurance that granting individuals access to Safeguards Information does not constitute an unreasonable risk to the public health and safety or the common defense and security.

background investigation (BI): information from all BI elements to be collectively evaluated by the reviewing official pursuant to make a determination of the trustworthiness and reliability of an individual. Depending on the BI period, the BI elements may include any or all of the following: verification of true identity, employment verification with suitable inquiry (includes education in lieu of employment and military service as employment), a credit check, and character and reputation determination.

barrel: the part of the firearm, usually made from iron or steel, through which the projectile(s) pass(es) when the firearm is fired.

barricade: a linear structure used as an obstacle or as support during the firing of a firearm.

behavior observation program (BOP): an awareness program that meets requirements of both the access authorization and fitness-for-duty programs. Personnel are trained to report legal actions; to possess certain knowledge and abilities (KAs) related to drugs and alcohol and the recognition of behaviors adverse to the safe operation and security of the facility by observing the behavior of others in the workplace and detecting and reporting aberrant behavior or changes in behavior that might adversely impact an individual's trustworthiness or reliability; and undergo an annual supervisory review.

best-effort: documented actions taken to verify the required employment, suitable inquiry, and education information pertaining to an individual's unescorted access authorization. Such actions are taken when the primary source fails to respond, refuses to assist, or indicates an inability or unwillingness to provide the requested information within 3 business days and a secondary source is used to complete the requirement.

bi-directional communications: transmission and receipt of data or signals between devices occurring in either direction along a communications medium at the same time. Transmission Control Protocol (TCP) is an example of bidirectional communications protocol.

bolt: a metal cylinder or block that drives the cartridge into the chamber of a firearm, locks the breech, and usually contains the firing pin and extractor.

bomb: an explosive device suspected of having sufficient force to damage plant systems or structures.

bore: the interior of the barrel, the diameter of which determines the caliber or gauge of the firearm.

boundary: a point of demarcation across that physically and logically separates defensive levels having different security requirements.

boundary interface: a boundary across which communication occurs between critical digital assets, systems, or networks contained within adjacent defensive levels.

breech: the part of the firearm to the rear of the bore that accepts ammunition.

bulk materials: products and materials with the following characteristics: large in quantity, volume, and mass; loose; not enclosed in separate packages or divided into separate parts. Bulk products and materials include but are not limited to the following examples: gravel, lumber, paving material, fill dirt, iron and steel pipe to include angles and sheets, gasoline, carbon dioxide, diesel fuel, hydrogen, nitrogen (liquid), power transformer oil, turbine oil, propane gas, sodium hydroxide, sulfuric acid, pressurized gas cylinders, and resins. Additional examples can be found in RG 5.76; NRC Package Search – Review Guideline Number 15, dated February 5, 1978; and Security Advisory 06-04, "Implementing Search Requirements and Approved Exceptions for Packages and Materials at NRC-Licensed Facilities," dated September 6, 2006.

bullet: the projectile that is expelled from a firearm when it is fired.

bullet-resisting (bullet/resisting): protection against complete penetration, passage of fragments of projectiles, and spalling (fragmentation) of the protective material that could cause injury to a person standing directly behind the bullet-resisting barrier.

business day: Monday through Friday, excluding federal holidays.

caliber: the diameter of the bore of a firearm or diameter of a bullet.

carbine: a compact, lightweight, short-barreled, rifled-bore, shoulder-fired firearm.

cartridge: a single piece of firearm ammunition consisting of casing, powder, primer, and projectile.

causal factors: those actions, conditions, or events which directly or indirectly influence the outcome of a situation or problem.

certification: documentation from an authorized supervisor/trainer attesting that an individual is qualified to perform a critical task.

certified: describes people who have received documentation from an authorized supervisor/trainer attesting that they are qualified to perform a critical task.

chamber: the part of the barrel's bore that holds the cartridge or a compartment in the cylinder of a revolver.

charge: to cause the action of a firearm to move, resulting in a cartridge being placed in the chamber and readied for firing.

circadian rhythm: the variation in human physiological processes that repeat on an approximate 24-hour cycle.

civil disturbance: a group of persons violently protesting station operations or activities at the site. This event does not involve hostile actions. Peaceful demonstrations are not civil disturbances.

clear: to ensure that a firearm has no cartridge in the chamber, cylinder, or loading mechanism and, if magazine-fed, that the magazine is also removed.

clip: a device used to hold multiple cartridges together. It is used as an aid in loading firearms' magazines or cylinders. It has no moving parts and is usually not retained in the firearm.

close-quarter battle: intensive combat situations at distances less than 21 feet, generally with multiple participants with firearms or other weapons or in hand-to-hand combat.

commercial off-the-shelf: software or hardware products that are ready-made and available for sale to the general public.

common-cause: describes multiple (i.e., two or more) failures of plant equipment or processes attributable to a shared cause.

compensate: to take measures, including using backup equipment, additional security personnel, specific procedures, or other actions taken to ensure that the effectiveness of the security systems is not reduced by failure or other contingencies affecting the operation of the security-related equipment, structures or processes. NRC-approved security plans and their associated implementing procedures normally describe preplanned compensatory measures.

compromised: sufficient evidence exists to verify that there is actual degradation of a security safeguards measure to the extent that it renders it ineffective for the intended purpose.

computer system: an electronic device that processes, retrieves, and stores programmed information or data.

contiguous sites: licensee-controlled locations deemed by the Commission to be in close enough proximity to each other that the special nuclear material must be considered in the aggregate for the purpose of physical protection.

contingency weapon: a firearm designated as the primary response weapon to be utilized by an armed responder or assigned armed security officer to defend the facility during an overt attack.

contingency plan: management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster

continuing training: training on critical tasks, conducted subsequent to initial training, as described in the Training and Qualification Plan, to ensure an individual maintains proficiency in performing the tasks.

contraband: firearms, explosives, incendiary devices or other items that may be carried or concealed by personnel, packages, materials or vehicles and could be used to commit radiological sabotage.

contractor/vendor (C/V): any company or any individual not employed by a licensee who is providing work or services to a licensee or other entity either by contract, purchase order, oral agreement, or other arrangement that supports the fulfillment of requirements related to unescorted access, unescorted access authorization, or fitness for duty.

contributing cause(s): any causes that by themselves would not create the problem, but are important enough to be recognized as needing corrective action.

controlled-access area: any temporarily or permanently established area which is clearly demarcated, access to which is controlled and which affords isolation of the material or persons within it.

corrective-action program: a formal system for handling problems raised by employees. Problems may require remedial action. Problems are tracked from their identification through evaluation and resolution. These issues are usually prioritized according to their relative safety significance.

countermeasure: an action, measure, or device that reduces risk.

course: an orderly progression of manipulating and shooting a firearm through specified stages and strings designed to exercise and evaluate firearm manipulation and shooting skills.

cover: protection from incoming projectiles.

credible: describes information received from a source determined to be reliable (e.g., law enforcement, government agency, U.S. Computer Emergency Response Team (CERT), etc.) or has been verified to be true. A threat can be verified to be true or considered credible when:

(1) evidence supporting the threat or vulnerability exists,

(2) information independent from the actual threat message or vulnerability exists that supports the threat or vulnerability, or

(3) a specific known group or organization claims responsibility for the threat or vulnerability.

critical digital asset (CDA): a subcomponent of a critical system that consists of or contains a digital device, computer, or communication system or network.

critical group: any individual who performs job functions that are critical to the safe and secure operation of the licensee's facility. This individual includes any individual who has been granted unescorted access or certified with unescorted access authorization and performs one or more of the following job functions:

a. has extensive knowledge of facility defensive strategies or designs and/or implements the plant's defense strategies;

b. in a position to grant an individual unescorted access or to certify an individual unescorted access authorization;

c. is assigned a duty to search for contraband (e.g., weapons, explosives, incendiary devices);

d. any individual who has the combination of electronic access AND the administrative control (e.g., "system administrator rights") to alter one or more security controls associated with one or more critical digital assets should be in the critical group.

e. also, any individual with extensive knowledge of the site-specific cyber defensive strategy should also be in the critical group.

"Extensive knowledge" is defined as having (a) knowledge of the cyber security controls in place for a critical digital asset (CDA), or (b) knowledge of how the configuration of a CDA or the cyber security controls can be modified in a manner that could result in an adverse impact to safety, important-to-safety, security, or emergency-preparedness (SSEP) functions.

Individuals performing the following functions should be included:

- site cyber security supervisors
- site cyber security manager
- site cyber security training manager
- corporate cyber security manager

"Administrative control" is defined as the electronic access and rights to independently change either the configuration of a CDA or the cyber security controls in place for a CDA, in a manner that could result in an adverse impact to SSEP functions.

Individuals performing the following functions should be included, as applicable:

- cyber security engineers and administrators
- information-technology personnel who are responsible for authorizing access to CDAs
- CDA system administrators
- personnel that can independently change the configuration of CDAs or can alter security controls

critical system (CS): an analog or digital technology-based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency-preparedness function. These critical systems include, but are not limited to, plant systems, equipment, communication systems, networks, offsite communications, or support systems or equipment that perform or are associated with a safety-related, important-to-safety, security, or emergency-preparedness function.

cumulative fatigue: the increase in fatigue over consecutive sleep-wake periods resulting from inadequate rest.

custodian: one who guards and protects or maintains, especially one entrusted with guarding and maintaining property or records.

cyber attack: the manifestation of either physical or logical (i.e., electronic or digital) threats against computers, communication systems, or networks that may (1) originate from either inside or outside the licensee's facility, (2) have internal and external components, (3) involve physical or logical threats, (4) be directed or non-directed in nature, (5) be conducted by threat agents having either malicious or non-malicious intent, and (6) have the potential to result in direct or indirect adverse effects or consequences to critical digital assets or critical systems. This includes attempts to gain unauthorized access to a critical digital asset's and/or critical system's services, resources, or information and attempts to cause an adverse impact to a safety, important-to-safety, security, or emergency-preparedness function. Further background on cyber attacks which are up and including the SBT, can be found in Sections 1.1(c), 1.2, and 1.5 of RG 5.69, "Guidance for the Application of Radiological Sabotage Design-Basis Threat in the Design, Development and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements." Cyber attacks may occur individually or in any combination.

cylinder: one of the rotating chambers of a revolver that hold the cartridges.

deadly force: that force capable of causing serious physical injury or death.

deceit: methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear materials, where the attempt involves falsification to present the appearance of authorized access.

defense in depth: an approach to security in which multiple levels of security and methods are deployed to guard against failure in one component or level.

degraded: describes the performance of a security safeguards measure that has been reduced to the degree that it is rendered ineffective for the intended purpose.

designated armed security officer: those armed security officers identified in the NRC-approved security plans to perform armed response force duties required by the protective strategy and are available at all times onsite to carry out armed response force duties as a member of the Armed Response Team.

desirable target sets: target sets that would be identified by an adversary as requiring the least resources to neutralize.

determination of fitness: a process designed to examine an individual when there are indications that the individual may be in violation of the licensee's or contractor/vendor's fitness-for-duty policy or is otherwise unable to safely and competently perform his or her duties.

DHS Consultation: independent assessment conducted by the Department of Homeland Security (DHS) of the potential vulnerabilities of a new reactor location to a terrorist attack. (Memorandum of Understanding, Section 657, "Department of Homeland Security Consultation," of the Energy Policy Act of 2005, Pub. L. 109-58, 119 Stat. 814 (2005))

discovery (time of): a specific time at which a supervisor or manager makes a determination that a verified degradation of a security safeguards measure or a contingency situation exists.

diversion of SNM (at any level): unauthorized removal or control of special nuclear material (SNM).

draw: to bring out a firearm, usually a handgun, from a holster worn on the body and direct it toward a target.

dry fire: to manipulate a firearm and practice firing with no live cartridges or to use inert ammunition (dummy rounds).

duress alarm: a method of alerting another that an individual is being subjected to compulsion through threat, illegal coercion, or forced restraint.

emergency conditions: abnormal conditions that could present a threat to the facility, personnel, or the general public if not mitigated.

employment action: a formal change in job responsibilities or removal from a job, or the employer-mandated implementation of a plan for substance abuse treatment in order to avoid a formal change in or removal from a job, or any military non-judicial punishment because of the individual's use of drugs or alcohol or violation of a fitness-for-duty policy.

employment/unemployment history verification: a check for specified periods of employment, military service as employment, education in lieu of employment, and unemployment on a best-effort basis from information claimed by the individual on their personal history questionnaire.

enhanced weapon: any short-barreled shotgun, short-barreled rifle, or machine gun. Enhanced weapons do not include destructive devices as defined in 18 U.S.C. 921(a). Enhanced weapons do not include standard weapons.

extent of cause: the extent to which the root causes of an identified problem have affected other plant processes, equipment, or human performance.

extent of condition: the extent to which the actual condition exists with other plant processes, equipment, or human performance.

false alarm: an alarm generated without an apparent cause.

fatigue: the degradation in an individual's cognitive and motor functioning resulting from inadequate rest.

fire: to discharge a firearm.

firearm: a weapon from which a projectile(s) is discharged by gunpowder, particularly small arms such as rifles or handguns.

fitness-for-duty (FFD) authorization: an element of unescorted access that identifies the status of an individual's required fitness-for-duty elements, which are then evaluated by a reviewing official to determine the individual's trustworthiness, reliability, and fitness for duty. These required elements for FFD authorization are: suitable inquiry (including education in lieu of employment and military service as employment), self-disclosure, pre-access drug and alcohol testing, and being subject to both a licensee-approved behavior observation and random drug and alcohol testing program.

force: violent methods used by an adversary to attempt to steal strategic special nuclear material or to sabotage a nuclear facility or violent methods used by response personnel to protect against such adversary actions.

force continuum (use-of-force continuum): a standard that provides individuals with guidelines as to how much force may be used against a resisting or combative subject in a given situation.

formal application: an individual is considered to have unescorted access authorization formally applied for the time the licensee or contractor/vendor initiates its first formal action satisfying any of the requirements for such authorization.

fratricide: the employment of friendly weapons and munitions, with the intent to neutralize the enemy or destroy his equipment or facilities, which results in unforeseen and unintentional death or injury to friendly personnel.

gauge: a measuring system used to determine the bore diameter of a shotgun barrel based on the number of balls of bore diameter that can be produced from a pound of lead.

grip: (verb) to place one or more hands on a firearm to permit effective firing.
(noun) the portion of a firearm designed for holding it in order to fire.

guard: a uniformed individual armed with a firearm whose primary duty is the protection of special nuclear material against theft, the protection of a plant against radiological sabotage, or both.

hammer: the part of a firearm that strikes the primer, firing pin, or percussion cap, causing the firearm to fire a projectile.

handgun: a firearm capable of being held and fired with one hand.

hazardous materials: materials of sufficient quantity and hazard as defined by the U.S. Department of Transportation (in 49 CFR 171.8, "Definitions and Abbreviations") to present a threat to the facility if used by an adversary for that purpose.

hijack: the act of surreptitiously or overtly controlling an analog or digital systems (e.g. equipment, computers, communications by an unauthorized user. Hijacking has the goal to modify, destroy, or compromise the integrity or confidentiality of data and/or computer programs(s), deny access to systems, services, and/or data; gain control of computer systems, including critical digital assets and or critical systems, or impact the operation of computer system(s), critical systems and/or critical digital assets, and/or support systems.

host-based intrusion-detection system (HIDS): an application that detects possible malicious activity on a host from characteristics such as change of files (file-system integrity checker), operating system call profiles, etc.

hostile action: an act toward a nuclear power plant or its personnel that includes the use of violent force to destroy equipment, take hostages, and/or intimidate the licensee to achieve an end. This includes attack by air, land, or water using guns, explosives, projectiles, vehicles, or other devices to deliver destructive force. Other acts that satisfy the overall intent may be included. Hostile action should not be construed to include acts of civil disobedience or felonious acts that are not part of a concerted attack on the nuclear power plant.

hostile force: one or more individuals who are engaged in a determined assault, overtly or by stealth and deception, equipped with suitable weapons capable of killing, maiming, or causing destruction.

inappropriate action/unsafe act: an action or inaction that changes a normal situation into an abnormal one.

imminent/impending: about to happen (generally within 30 minutes).

imminent security threat authority: an NRC senior manager with the designated authority to issue immediately effective orders, including oral orders, to one or more licensees in the event of an imminent security threat, in accordance with Section 2.202, "Orders," of Title 10, "Energy," of the *Code of Federal Regulations*.

incident: occurrence, caused by either human action or natural phenomena, that may cause harm and that may require action.

incendiary device: any self-contained device intended to create an intense fire that can damage normally flame-resistant or -retardant materials.

identifiable: means that there is adequate information or a means to provide this information on the location and function of the cable target element (e.g., from labels, observation

through walk down, preexisting analysis, site documentation, etc.) and that the cable target element can be visually recognized by an adversary.

individual authorized access to Safeguards Information: a person permitted to have access to and handle such information pursuant to Safeguards Information under the requirements of 10 CFR 73.21, "Protection of Safeguards Information: Performance Requirements," and 10 CFR 73.22, "Protection of Safeguards Information: Specific Requirements."

individual authorized access to Safeguards Information: Modified Handling: a person permitted to have access to and to handle Safeguards Information designated as Safeguards Information: Modified Handling information pursuant to the requirements of 10 CFR 73.21 and 10 CFR 73.23, "Protection of Safeguards Information: Modified Handling: Specific Requirements."

initial unescorted access authorization: an access category used to identify persons in the process of obtaining unescorted access (UA) at a nuclear power plant for the first time, or after a lapsed clearance beyond the established 3-year cutoff, or after the most recent UA or unescorted access authorization was denied or terminated unfavorably as defined in Section 6.2 of NEI 03-01.

insider: a person who has been granted unescorted access or unescorted access authorization under the requirements of 10 CFR 73.56, "Personnel Access Authorization Requirements for Nuclear Power Plants," or has the ability to access information systems that: (1) connect to systems that connect to plant operating systems; or (2) contain sensitive information that may assist an insider in an attempted act of sabotage.

integrity: quality of a system reflecting the logical correctness and reliability of the operation of the system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Additionally, integrity includes protection against unauthorized modification or destruction of information.

interruption of normal operations: a departure from normal operation or condition that, if accomplished, would challenge the plant safety systems. This may also include an event that causes a significant redistribution of security or safety resources. This could include intentional tampering with systems or equipment that is normally in standby but would need to operate if called upon.

intrusion: a person(s) present in a specified area without authorization. Discovery of a bomb in a specified area is an indication of intrusion into that area by a hostile force.

intrusion alarm: a tamper-indicating electrical, electromechanical, electro-optical, electronic, or similar device which will detect intrusion by an individual into a building, protected area, vital area, or material access area, and alert guards or watchmen by means of actuated visible and audible signals.

Intrusion Detection System (IDS): a system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include intrusions, misuse, unauthorized access, or malicious or abnormal operation. These systems may be network- or host-based. Intrusion-detection functions include monitoring and analyzing both user and system activities, analyzing system configurations and vulnerabilities, assessing system and file integrity, recognizing patterns typical of attacks, analyzing abnormal activity patterns, and tracking user policy violations.

Intrusion-Prevention System (IPS): an intrusion-detection system that has the ability to take actions to preempt or stop activities identified as malicious.

isolation zone: any area adjacent to a physical barrier, clear of all objects which could conceal or shield an individual.

jamming: to make it difficult or impossible to receive desired communication signals. A jamming signal may be intended to block a single frequency (called "spot jamming") or to block a band of frequencies (called "barrage").

knowledgeable and practiced (K&P): describes an individual audit team member who has current or previous access authorization program experience and who is responsible for validating that overall program performance is meeting the objective of screening individuals to provide high assurance that individuals are trustworthy and reliable to have or keep unescorted access or unescorted access authorization.

large aircraft: aircraft used for long-distance flights from coast to coast in the United States.

law enforcement response plan: a documented plan that describes support from local, state, and Federal law enforcement agencies expected to immediately respond to incidents, including the communication methodologies and protocols, command and control structure, marshaling locations, estimated response times, anticipated response capabilities, and specialized equipment to be used.

legal action: a formal action taken by a law enforcement authority or court of law, including being held, detained, taken into custody, charged, arrested, indicted, or fined; having bond forfeited; or being cited or convicted for a violation of any law, regulation, or ordinance (e.g., felony, misdemeanor, traffic violation, military criminal history, etc.), or the mandated implementation of a plan for treatment or mitigation in order to avoid a permanent record of an arrest or conviction in response to the following activities:

(1) The use, sale or possession of illegal drugs

(2) The abuse of legal drugs or alcohol; or

(3) The refusal to take a drug or alcohol test.

lock: 1. lock/locked: secured by a three-position, manipulation resistant, dial type, built-in combination lock or combination padlock and in the case of fences, walls, and buildings

means an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock or electromechanical device which provides the same function.

2. lock in the case of vaults or vault type rooms: a three-position, manipulation resistant, dial type, built-in combination lock or combination padlock and in the case of fences, walls, and buildings means an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock. Lock in the case of a vault or vault type room also means any manipulation resistant, electromechanical device which provides the same function as a built-in combination lock or combination padlock, which can be operated remotely or by the reading or insertion of information, which can be uniquely characterized, and which allows operation of the device. Locked means protected by an operable lock. *for fences, walls, or buildings*, an integral door lock or padlock which provides protection equivalent to a six-tumbler cylinder lock.

magazine: a component in some types of firearms (occasionally a detachable metal box) in which cartridges are placed. The magazine contains a spring and a follower and is part of the mechanism by which cartridges are fed into the chamber.

maintenance: onsite activities that include, for the purposes of 10 CFR 26.4(a)(4): modification, surveillance, post maintenance testing, and corrective and preventive maintenance.

malicious/malevolent intent: intentionally causing harm, damage, or injury or to disrupt normal operation within the facility.

malware: malicious software designed to infiltrate or damage a CDA without the licensee's or applicant's consent. Malware is taken to include computer viruses, worms, Trojan horses, Root kits, spyware, and adware.

material access area: any location containing special nuclear material within a vault or building, the roof, walls, and floor of which each constitute a physical barrier.

medical review officer (MRO): a licensed physician who is responsible for receiving laboratory results generated by a drug testing program conducted in accordance with 10 CFR Part 26, "Fitness for Duty Programs," and who has the appropriate medical training to properly interpret and evaluate an individual's drug and validity test results together with his or her medical history and any other relevant biomedical information.

memorandum of understanding (MOU): a document detailing an agreement between the licensee and outside law enforcement agencies (at all levels) or emergency service agencies (e.g., firefighting, decontamination, or medical) for augmentation of site security and safety emergency response or compensatory actions taken to appropriate onsite events (e.g., personnel, equipment, or professional assistance).

mobile code: programs or parts of programs obtained from remote control systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

muzzle: the discharge end of a barrel.

need to know: a determination by a person having responsibility for protecting Safeguards Information (including Safeguards Information designated as Safeguards Information: Modified Handling) that a proposed recipient's access to Safeguards Information is necessary in the performance of official, contractual, licensee, applicant, or certificate holder employment. In an adjudication, ''need to know'' means a determination by the originator of the information that the information is necessary to enable the proposed recipient to proffer and/or adjudicate a specific contention in that proceeding, and the proposed recipient of the specific Safeguards Information possesses demonstrable knowledge, skill, training, or education to effectively utilize the specific Safeguards Information in the proceeding. Where the information is in the possession of the originator and the NRC staff (dual possession), whether in its original form or incorporated into another document or other matter by the recipient, the NRC staff makes the determination. In the event of a dispute regarding the ''need to know'' determination, the presiding officer of the proceeding shall make the ''need to know'' determination.

network: group of components that share information or interact with each other in order to perform a function.

nuisance alarm: an alarm generated by an identified input to a sensor or monitoring device that does not represent a safeguards threat and is not a result of normal authorized activity. Nuisance alarms may be caused by environmental conditions (e.g., rain, sleet, snow, or lightning) or mechanical conditions (e.g., natural objects such as animals or tall grass).

operability testing: testing to ensure that equipment components are energized and that visual and audible indications are functioning properly.

other items: items that have an apparent primary use as a weapon (e.g., crossbows, brass knuckles, swords, nunchucks, etc.) or destructive devices as defined in 26 U.S.C. 5845(f) intended for use in the commission of radiological sabotage. Other items do not include ordinary tools or materials routinely used in the operation and maintenance of a commercial nuclear power reactor facility that could potentially be used in a manner for which they are not intended.

passive insider: a person who provides or attempts to provide Safeguards Information or other relevant information regarding a licensee's physical configurations, designs, strategies, or capabilities to any person who does not have a functional or operational need to know.

passive vehicle barrier: a barrier used as appropriate, for those portions of the vehicle barrier system (VBS) that are not needed for vehicle access. The passive barriers may make use of natural topographical features and structures provided these features and structures, along with other segments of the barrier, provide a continuous vehicle barrier against land access to the facility. In considering a barrier, natural features or devices that limit or channel vehicle direction and speed also may be appropriate to simplify or reduce the performance required of the VBS.

patch: a fix for a critical digital asset or software program where the actual binary executable and related files are modified.

performance testing: to test to ensure the design stimulus will be detected properly.

person:

(1) any individual, corporation, partnership, firm, association, trust, estate, public or private institution, group, government agency other than the Commission or the Department of Energy (DOE), (except that the DOE shall be considered a person to the extent that its facilities are subject to the licensing and related regulatory authority of the Commission pursuant to section 202 of the Energy Reorganization Act of 1974 and sections 104, 105, and 202 of the Uranium Mill Tailings Radiation Control Act of 1978), any state or political subdivision of a state, or any political subdivision of any government or nation, or other entity; or

(2) any legal successor, representative, agent, or agency of the foregoing.

personal history questionnaire (PHQ): information provided in a written statement by an individual applying for unescorted access authorization (UAA) that provides the personal information required to assist in processing unescorted access or UAA elements.

personal information: all information unique to an individual that is collected or developed during the implementation of unescorted access authorization or fitness-for-duty program requirements.

physical barrier:

(1) fences constructed of No. 11 American Wire Gauge or heavier wire fabric, topped by three strands or more of barbed wire or similar material on brackets angled inward or outward between 30° and 45° from the vertical, with an overall height of not less than 8 feet, including the barbed topping;

(2) building walls, floors, and ceiling constructed of stone, brick, cinder block, concrete, steel, or comparable materials (openings in which are secured by grates, doors, or covers of construction and fastening of sufficient strength such that the integrity of the wall is not lessened by any opening), or walls of similar construction, not part of a building, provided with a barbed topping described in definition of a height of not less than 8 feet; or

(3) Any other physical obstruction constructed in a manner and of materials suitable for the purpose for which the obstruction is intended.

Physical Security Inspections, Tests, Analyses, and Acceptance Criteria (PS-ITAAC): activities conducted to provide reasonable assurance that the physical security hardware associated with the facility has been constructed and will be operated in conformity with the facility's license before operation of the facility. Features of a facility that are subject to PS-ITAAC include, but are not limited to, communication systems, assessment and

alarm systems, locks, personnel access control, physical equipment barriers, and surveillance devices. (Section 14.3.12, "Physical Security Hardware - Inspections, Tests, Analyses, and Acceptance Criteria," of NUREG-0800, "Standard Review Plan")

pistol: a handgun with a chamber that is integral with the barrel.

player: individuals must participate in one of the following roles to satisfy this requirement as a player (i.e. response team leaders, alarm station operators, armed responders, armed security officers designated as a component of the protective strategy).

position description: a statement or description outlining the essential functions of a job and the potential exposures and hazards associated with those functions, or the environment in which the functions are executed.

potentially disqualifying information (PDI): any derogatory information (e.g., unfavorable information from an employer, developed or disclosed criminal history, credit history such as but not limited to collection accounts, bankruptcies, tax liens, and judgments), unfavorable reference information, evidence of drug or alcohol abuse, discrepancies between information disclosed and developed) that is required to be evaluated against a licensee's or contractor/vendor's (C/V's) adjudication criteria. A subset of PDI is fitness-for-duty (FFD) PDI (the 10 CFR Part 26 equivalent of which is PDFFDI, Potentially Disqualifying Fitness-for-Duty Information) and includes information demonstrating that an individual has:

(1) Violated a licensee's or approved C/V's FFD policy;

(2) Had authorization denied or terminated unfavorably from or made ineligible for unescorted access to any nuclear facility, Technical Support Center, or Emergency Operations Facility for a violation of a fitness-for-duty program; falsification of employment or self-disclosure statement; the sale, use, or possession of illegal drugs; or the consumption of alcohol within a protected area of a nuclear power plant;

(3) Used, sold, or possessed illegal drugs;

(4) Abused legal drugs or alcohol;

(5) Subverted or attempted to subvert a drug or alcohol testing program;

(6) Refused to take a drug or alcohol test;

(7) Been subjected to a plan for substance-abuse treatment (except for self-referral); or

(8) Had legal action or employment action taken against him or her for alcohol or drug use.

pre-event notification period: the period between the point at which licensees are notified of a potential aircraft threat and when an onsite impact occurs.

preventive action: an action taken in response to an adversary attack to prevent significant core damage and/or prevent an offsite release.

print: perforation on a target caused by a projectile.

problem: a term synonymous with condition, event, or concern, and any other failure, malfunction, deficiency, or deviation, and defective equipment and nonconformance in security program components and functions. In addition, "problem" includes inappropriate security personnel actions that may be detrimental to nuclear, personnel, and environmental safety.

prohibited items: items that are not relative to the conduct of work or that do not serve a purposeful function within the environment and are considered contrary to safety and security. Such items could be used to adversely affect personnel, systems, or equipment required to protect special nuclear material.

projectile: a fired, projected object, such as a bullet or pellet having no capacity for self-propulsion, directed toward a nuclear power plant that could cause concern for the plant's continued operability, reliability, or personnel safety.

protected area: an area encompassed by physical barriers and to which access is controlled.

qualification: an individual has received appropriate training and has demonstrated through written examination or practical demonstration that he or she is able to effectively perform the task(s) assigned.

quarterly: scheduled at a nominal 13-week periodicity. Performance may be conducted up to four weeks before to four weeks after the scheduled date. The next scheduled date is 13 weeks from the originally scheduled date.

radiological sabotage: any deliberate act directed against a plant or transport in which an activity licensed pursuant to 10 CFR Part 73 of NRC's regulations is conducted, or against a component of such a plant or transport which could directly or indirectly endanger the public health and safety by exposure to radiation. (10 CFR 73.2 and http://www.nrc.gov/reading-rm/basic-ref/glossary/radiological-sabotage.html)

recovery: steps taken to restore a system, function, or device to its original state of operation following a catastrophic or partial loss of functionality or when an original state of operation is challenged by either an event (such as a cyber attack) or anomaly (behavior not expected from normal operation).

reinstatement of unescorted access authorization: an unescorted access authorization that has been reestablished within 365 days consistent with unescorted access authorization requirements specified in Sections 6.4 and 6.5 of NEI 03-01.

reinvestigation: a periodic inquiry or assessment conducted to ensure that individuals continue to meet unescorted access, unescorted access authorization, or fitness-for-duty program suitability requirements as defined in the latest version of NEI 03-01 that describes an approach that the NRC staff has found acceptable.

remote access: the ability to access a critical digital asset (CDA), computer, node, or network resource located within an identified defensive level from a CDA, computer, or node that is physically located in a less secure defensive level.

remotely operated weapons system (ROWS): a weapons system that is operated from a remote location and typically includes a support structure and operator control station.

repeat occurrences: two or more independent conditions which are the result of the same basic cause(s).

response team leader (RTL): the individual responsible for directing designated members of the security force in effecting the protective strategy at the facility. The response team leader is designated by the protective strategy and identified in facility procedures.

reviewing official: the licensee or, if applicable, contractor/vendor (C/V) designated by their company to be responsible for reviewing and evaluating all data collected about an individual, including potentially disqualifying information, in order to determine whether the individual may be certified for unescorted access authorization by a licensee or C/V or granted unescorted access by a licensee.

revolver: a handgun with a cylinder of multiple chambers brought successively into line with the barrel and discharged by the same hammer.

rifle: a shoulder-fired firearm with a rifled barrel designed for single-shot, semiautomatic, or full-automatic firing.

root cause(s): the basic reason(s) (e.g., hardware, process, or human performance) for a problem which, if corrected, will prevent recurrence of that problem.

round: common term for a single firearm cartridge.

ROWS operator: an armed member of the security organization who:

- is trained and qualified as an armed responder and armed security officer and is designated to respond to a contingency event;
- is trained and qualified to operate remotely operated weapons systems (ROWS);
- has the primary responsibility of responding to threats against the facility up to and including the design-basis threat; and
- may be assigned other duties that do not prevent them from effectively responding in accordance with the protective strategy. They are not assigned any other duties that would impede an effective response).

safe shutdown: the ability to safely reduce reactor power to a stable and maintainable status while preserving the integrity of the fuel.

safeguards: this term has historically referred to the two major components of the NRC and internationally required protective components: material control, accounting, and security. "Security" usually refers to physical or procedural means of preventing harm to the assets of a facility. "Safeguards" may also have specific contextual meaning such as "Safeguards Information" or "safeguards event log."

safeguards contingency: a security-related event that presents a threat to the facility, its personnel, or the public and requires a response in accordance with the Contingency.

safeguards information: information not classified as National Security Information or Restricted Data which specifically identifies a licensee's or applicant's detailed control and accounting procedures for the physical protection of special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; detailed security measures (including security plans, procedures, and equipment) for the physical protection of source, byproduct, or special nuclear material in quantities determined by the Commission through order or regulation to be significant to the public health and safety or the common defense and security; security measures for the physical protection of and location of certain plant equipment vital to the safety of production or utilization facilities; and any other information within the scope of Section 147, "Safeguards Information," of the Atomic Energy Act of 1954, as amended, the unauthorized disclosure of which, as determined by the Commission through order or regulation, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of sabotage or theft or diversion of source, byproduct, or special nuclear material.

safeguards information: modified handling: the designation or marking applied to Safeguards Information which the Commission has determined requires handling requirements modified from the specific Safeguards Information handling requirements that are applicable to Safeguards Information needing a higher level of protection.

sanitization: a process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

scope: an optical instrument used to aid the human eye in sighting a firearm.

security management: persons responsible for security at the policy and general management level.

security monitoring network: a physically separated network that is provided to support the cyber security infrastructure with an equal or greater security level than the security levels it is supporting.

security officer: a uniformed individual, either armed with a covered weapon or unarmed, whose primary duty is the protection of the facility, of radioactive material, or of other property against theft or diversion or against radiological sabotage.

security-related: depending on the context in which it is used: (1), directly associated with the security systems, personnel, or plans, or (2) directly associated with a security threat to the facility.

security response: as used in this guide this means the substantive implementation of the armed response capabilities.

security storage container:
(1) *for storage in a building located within a protected or controlled-access area* -a steel filing cabinet equipped with a steel locking bar and a three-position General Service Administration (GSA)-approved padlock with a changeable combination;
(2) a security filing cabinet that bears a Test Certification Label on the side of the locking drawer or on the interior plate and is marked "General Services Administration Approved Security Container" on the exterior of the top drawer or door;
(3) a bank safe-deposit box; or
(4) another repository which in the judgment of the NRC would provide comparable physical protection.

security supervision: persons, not necessarily uniformed or armed, whose primary duties are supervision and direction of security at the day-to-day operating Removed. This might include:

- **security shift supervisor**: an individual responsible for ensuring that security force personnel assigned to their shift perform their duties and responsibilities as intended and consistent with NRC requirements, site plans, and site procedures; ensuring that there are an adequate number of qualified armed response team members and other security personnel available to effectively support both the normal operations and implementation of the site protective strategy; and monitoring on-duty security force members for fitness-for-duty requirements under 10 CFR 26.

- **security supervisor**: is (as referred to in Appendix B, "Training and Qualification Plan") an individual serving in a position defined by licensee directives as being responsible for attesting to training documentation. The supervisor may be either a proprietary or contracted employee who has been formally designated as a Security Supervisor.

security system: the compilation of all elements that make up the physical protection program necessary to meet 10 CFR Part 73 requirements, such as equipment, personnel, procedures, and personnel practices, to include the way in which each element interacts with and effects other elements.

self-disclosure: an individual applying for unescorted access authorization is required to report criminal and fitness-for-duty personal information in a personal history questionnaire that is verified during the background investigation and evaluated relative to the individual's trustworthiness, reliability, and fitness for duty. Also, as required while in a behavioral observation program, the individual is required to report all arrests at the time of occurrence.

self-checking: providing automatic monitoring and an indication if a system is not performing its intended function.

semi-automatic: a firearm using gas pressure or force of recoil and mechanical spring action to complete one cycle of the firing sequence (fire, unlock, extract, eject, cock, feed, chamber, lock) with a single pull of the trigger. The trigger must be released and re-pressed to begin a second firing sequence.

semi-structured interview: an interview with an individual applying for unescorted access authorization or a person maintaining unescorted access authorization, conducted by a psychiatrist or a licensed psychologist with clinical experience as required by applicable state requirements, containing questions determined appropriate by the interviewing psychiatrist or licensed psychologist which vary the focus and content of the interview, depending on the written assessment, the observations of the interviewer, and the interviewee's responses to questions. The semi-structured interview may contain any other evaluative measure determined appropriate by the psychiatrist or licensed psychologist.

shot: a projectile, such as a bullet or pellet, from a firearm. This term typically refers to small, round pellets fired from a shotgun.

shotgun: a smooth-bore shoulder firearm for firing single (slug) or multiple projectiles (pellets), usually at moderate distance.

sight alignment: correct positioning of the front sight within the center space of the rear sight. For firearms equipped with a scope, the scope must be aligned with the bore before shooting.

sight picture: correct alignment of the target with the correctly aligned sight(s) to ensure that a projectile strikes the target at the point of aim.

significant core damage: non-incipient, non-localized fuel melting and/or core destruction.

single act: an adversarial act, bounded by the design-basis threat, initiated in the owner-controlled area (OCA) or at the protected area (PA) perimeter, that would simultaneously remove the ability of both the central alarm station (CAS) and secondary alarm station (SAS) to (1) detect and assess alarms, (2) initiate and coordinate an adequate response to an alarm, (3) summon offsite assistance, or (4) provide command and control as specified in 10 CFR 73.55(i)(4)(i) (e.g., if detection and assessment of alarms are removed from both the CAS and SAS by a single adversarial action, the licensee would not be in compliance with the rule). One alarm station must be able to provide all four of these capabilities following a single act. The Commission's requirement to protect against a single act is satisfied upon adversary detection and initiation of the site protective strategy.

sleep debt: the difference between the amount of sleep in individual needs and the amount of sleep that the individual actually obtains.

slug: an elongated projectile of bore diameter for a shotgun that may have a hollow base and spiral driving bands (rifling) on its surface.

small aircraft: general aviation aircraft, rotary-wing aircraft (i.e., helicopters), or other small aviation assets (e.g., ultralights, gliders, civilian experimental aircraft).

special nuclear material of low strategic significance: (1) Less than an amount of special nuclear material of moderate strategic significance as defined in paragraph 1 of the definition of strategic nuclear material of moderate strategic significance in this section, but more than 15 grams of uranium-235 (contained in uranium enriched to 20 percent or more in U-235 isotope) or 15 grams of uranium-233 or 15 grams of plutonium or the combination of 15 grams when computed by the equation, grams = (grams contained U-235) + (grams plutonium) + (grams U-233); or (2) Less than 10,000 grams but more than 1,000 grams of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U-235 isotope); or (3) 10,000 grams or more of uranium-235 (contained in uranium enriched above natural but less than 10 percent in the U-235 isotope). This class of material is sometimes referred to as a Category III quantity of material.

special nuclear material of moderate strategic significance: (1) Less than a formula quantity of strategic special nuclear material but more than 1,000 grams of uranium-235 (contained in uranium enriched to 20 percent or more in the U-235 isotope) or more than 500 grams of uranium-233 or plutonium, or in a combined quantity of more than 1,000 grams when computed by the equation, grams = (grams contained U-235) + 2 (grams U-233 + grams plutonium); or (2) 10,000 grams or more of uranium-235 (contained in uranium enriched to 10 percent or more but less than 20 percent in the U-235 isotope). This class of material is sometimes referred to as a Category II quantity of material. (10 CFR 73.2)

specific: (in the context of a threat) the threat is related directly to the facility.

spent fuel sabotage: a loss of spent fuel pool coolant inventory and exposure of spent fuel, barring extraordinary actions by plant operations.

stage: a segment of a firearms qualification course which may consist of one or more strings using similar techniques at a specified distance.

stealth: methods used to attempt to gain unauthorized access, introduce unauthorized materials, or remove strategic special nuclear material, where the fact of such attempt is concealed or an attempt is made to conceal it.

strategic special nuclear material: uranium-235 (U-235) contained in uranium enriched to 20 percent or more in the U-235 isotope, uranium-233, or plutonium.

string: a segment of a stage in a firearms course, usually a continuous series of shots fired within a specified time limit.

substance-abuse expert (SAE): an individual who meets the requirements of 10 CFR 26.187, “Substance Abuse Expert,” and is relied on to make a determination of fitness.

suitable inquiry (SI): a best-effort verification of self-disclosed fitness-for-duty (FFD) information and an employment history check, which is obtained by questioning previous employers and/or educational institutions to determine if the individual was, in the past:

- tested positive for illegal drugs;
- subject to a plan to treat substance abuse (except after self-referral);
- removed from, or made ineligible for, activities within the scope of 10 CFR 26; or
- denied unescorted access or unescorted access authorization at any nuclear power plant or other employment with a FFD policy.

supplemental security officers: trained and qualified armed security officers who are present in numbers beyond the minimum committed number of armed responders or armed security officers. They may be available onsite to respond to threats against the facility and may be assigned to any duty, as they are not required nor relied on for immediate response by the protective strategy.

support equipment: equipment that directly or indirectly supports the operation or functionality of systems associated with safety, important-to-safety, security, or emergency-preparedness functions and if compromised, the equipment could adversely impact safety, important to safety, security or emergency preparedness functions. Examples of support equipment include, but are not limited to, handling, testing and maintenance equipment and parts, which if compromised could have an adverse impact on the safety, important to safety, security or emergency preparedness functions.

support system: a system that directly or indirectly supports the operation or functionality of systems associated with safety, important-to-safety, security, or emergency-preparedness functions and if compromised, the system could adversely impact safety, important to safety, security or emergency preparedness functions. Examples of support system include, but are not limited to, electrical power, heating, ventilation, and air conditioning, communications, fire suppression, or any system, which if compromised could have an adverse impact on the safety, important to safety, security or emergency preparedness functions.

tactical response team: the primary response force for each shift which can be identified by a distinctive item of uniform, armed with specified weapons, and whose other duties permit immediate response.

tamper-indicating: providing a visual or audible means of identifying unauthorized use of manipulation.

tampering: deliberately damaging, disabling, or altering equipment necessary for safe shutdown or security equipment necessary for the protection of the facility in order to defeat their function and/or prevent them from operating.

target area: the close vicinity to the location of one or more target elements.

target element: structures, systems, or components or operator actions that perform a function to prevent significant core damage or spent fuel damage and is included within the licensee's protective strategy.

target set: the minimum combination of equipment or operator actions which, if all are prevented from performing their intended safety function or prevented from being accomplished, would likely result in significant core damage (e.g., nonincipient, nonlocalized fuel melting and/or core destruction) or a loss of spent fuel pool coolant inventory and exposure of spent fuel, barring extraordinary actions by plant operations.

target set characterization: target set characterization is the evaluation of information related to target sets for the purpose of identifying targets that would appear desirable to the adversary.

terminated favorably: describes unescorted access authorization or unescorted access that has been terminated because it is no longer required. The individual was determined to be trustworthy and reliable and fit for duty up to the point in time that the termination occurred.

terminated unfavorably: the describes unescorted access authorization (UAA) or unescorted access (UA) that has been terminated because the licensee has determined that the individual cannot be considered trustworthy and/or reliable to hold UAA/UA, is unfit for duty, or has violated an access-authorization or fitness-for-duty policy.

theft of SNM: the unauthorized taking or controlling of special nuclear material (SNM) for unauthorized use.

threat: natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

threat type: one of three categories of aircraft threat based on specific criteria: "imminent," "probable," or "informational."

training cycle: a period over which the continuing training program is conducted and evaluated (normally over a three year period).

trustworthiness and reliability: are characteristics of an individual considered dependable in judgment, character, and performance, such that disclosure of Safeguards Information (including Safeguards Information designated as Safeguards Information: Modified Handling) to that individual does not constitute an unreasonable risk to the public health and safety or common defense and security. A determination of trustworthiness and reliability for this purpose is based upon a background check.

unauthorized person: any person who gains unescorted access to any area to which the person has not been properly authorized or gained unescorted access. This includes otherwise authorized persons who gain access in an unauthorized manner such as circumventing established access-control procedures by tailgating another authorized person.

unescorted access (UA): Granted to an individual after satisfactorily completing all regulatory requirements for unescorted access authorization and fitness-for-duty authorization, plant access training; is subjected to a behavioral observation program; is placed in a random drug and alcohol testing program; and is provided the physical means to gain UA to the protected area.

unescorted access authorization (UAA): Certification and status in the access authorization process that the individual satisfactorily completed all required elements as specified in Section 6 (including these fitness-for-duty authorization elements: consent, self-disclosure, suitability inquiry, and drug and alcohol testing elements defined in 10 CFR 26; being subject to a behavior-observation program; and training in the fitness-for-duty knowledge and abilities), evaluated by a licensee reviewing official who then made a favorable determination relative to the individual's trustworthiness, reliability, and fitness for duty.

updated unescorted access authorization: an unescorted access or unescorted access authorization that has been restored after authorization was terminated under favorable conditions during a period greater than 365 days but less than 3 years prior to restoration as specified in Section 6.3 of NEI 03-01.

vandalism: deliberate, malicious damage to equipment or property that is not related to safe shutdown or security equipment necessary for the protection of the facility. Damage may not render the component nonfunctional but results in actions that must be performed to restore original condition.

vault: a windowless enclosure with walls, a floor, a roof, and door(s) designed and constructed to delay penetration from forced entry.

vault-type room: a room with one or more doors, all capable of being locked, protected by an intrusion alarm which creates an alarm upon the entry of a person anywhere into the room and upon exit from the room or upon movement of an individual within the room.

visitor: an individual, not possessing unescorted access authorization (UAA), who is permitted to enter the Protected or Vital areas while escorted by an individual that does possess UAA.

vital area: any area that contains vital equipment.

vital equipment: any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital.

vulnerability: feature, attribute or weakness in a system's design, implementation, or operation and management that could render a critical digital asset open to exploitation or a safety, important-to-safety, security, or emergency-preparedness function susceptible to adverse impact.

watchman or watchperson: an individual, not necessarily uniformed or armed with a firearm, who provides protection for a plant and the special nuclear material therein in the course of performing other duties.

zero: to adjust a firearm's sighting mechanism(s) to cause a projectile to strike a target at the point of aim. This term may also refer to the number before 1

REFERENCES

1. *U.S. Code of Federal Regulations*, "Definitions," Section 73.2 of "Domestic Licensing of Production and Utilization Facilities," Part 50, Chapter I, Title 10, "Energy."

2. Nuclear Energy Institute (NEI), "Nuclear Power Plant Access Authorization Program," NEI 03-01, Revision 3, Washington, DC, May 2009.

3. NEI, "Template for the Security Plan, Training and Qualification Plan, Safeguards Contingency Plan, [and Independent Spent Fuel Storage Installation Program]," NEI 03-12, Revision 7, Washington, DC, October 2011.

4. U.S. Nuclear Regulatory Commission, "Response Strategies for Potential Aircraft Threats," Regulatory Guide (RG) 1.214.

5. U.S. Nuclear Regulatory Commission, "Standard Format and Content of Safeguards Contingency Plans for Nuclear Power Plants," RG 5.54.

6. U.S. Nuclear Regulatory Commission, "Access Authorization Program for Nuclear Power Plants," RG 5.66.

7. U.S. Nuclear Regulatory Commission, "Guidance for the Application of the Radiological Sabotage Design-Basis Threat in the Design, Development, and Implementation of a Physical Security Program that Meets 10 CFR 73.55 Requirements," RG 5.69.

8. U.S. Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Facilities," RG 5.71.

9. U.S. Nuclear Regulatory Commission, "Physical Security Hardware Inspections, Testing, Analyses, and Acceptance Criteria," RG 5.72.

10. U.S. Nuclear Regulatory Commission, "Fatigue Management for Nuclear Power Plant Personnel," RG 5.73.

11. U.S. Nuclear Regulatory Commission, "Managing the Safety/Security Interface," RG 5.74.

12. U.S. Nuclear Regulatory Commission, "Training and Qualification of Security Personnel at Nuclear Power Reactor Facilities," RG 5.75.

13. U.S. Nuclear Regulatory Commission, "Physical Protection Program at Nuclear Power Reactors," RG 5.76.

14. U.S. Nuclear Regulatory Commission, "Insider Mitigation Program," RG 5.77.

15. U.S. Nuclear Regulatory Commission, "Target Set Identification and Development for Nuclear Power Reactors," RG 5.81.

16. U.S. Nuclear Regulatory Commission, “IT Functions for the Critical Group,” Security Frequently Asked Question 10-05, October 2010.

17. U.S. Nuclear Regulatory Commission, “Glossary.” Available at <http://www.nrc.gov/reading-rm/basic-ref/glossary.html>, accessed January 31, 2014.

18. Memorandum of Understanding, Section 657, “Department of Homeland Security Consultation,” of the Energy Policy Act of 2005, Pub. L. 109-58, 119 Stat. 814 (2005).

19. U.S. Nuclear Regulatory Commission, “Physical Security Hardware - Inspections, Tests, Analyses, and Acceptance Criteria,” Section 14.3.12 of “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition,” NUREG-0800, Revision 1, Agencywide Documents Access and Management System (ADAMS) Accession No. ML100970568.

NRC FORM 335
(12-2010)
NRCMD 3.7

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

(See instructions on the reverse)

1. REPORT NUMBER
(Assigned by NRC, Add Vol., Supp., Rev., and Addendum Numbers, if any.)

NUREG-2203

2. TITLE AND SUBTITLE

Glossary of Security Terms for Nuclear Power Reactors

3. DATE REPORT PUBLISHED

MONTH	YEAR
February	2017

4. FIN OR GRANT NUMBER

5. AUTHOR(S)

Kris Jamgochian
Amy Roundtree
Wayne Chalk

6. TYPE OF REPORT

Technical

7. PERIOD COVERED (Inclusive Dates)

8. PERFORMING ORGANIZATION - NAME AND ADDRESS (If NRC, provide Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address; if contractor, provide name and mailing address.)

Division of Security Policy
Office of Nuclear Security and Incident Response
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

9. SPONSORING ORGANIZATION - NAME AND ADDRESS (If NRC, type "Same as above", if contractor, provide NRC Division, Office or Region, U. S. Nuclear Regulatory Commission, and mailing address.)

Same as above.

10. SUPPLEMENTARY NOTES

11. ABSTRACT (200 words or less)

This is a glossary of security terms specifically for nuclear power reactors that are commonly used in the nuclear industry and regulatory community. These terms were compiled from U.S. Nuclear Regulatory Commission and nuclear industry sources. This is published to assist agency authors, readers, and stakeholders in understanding common terms used in security.

12. KEY WORDS/DESCRIPTORS (List words or phrases that will assist researchers in locating the report.)

Security Terms
Glossary
Nuclear Power Plants.

13. AVAILABILITY STATEMENT

unlimited

14. SECURITY CLASSIFICATION

(This Page)
unclassified

(This Report)
unclassified

15. NUMBER OF PAGES

16. PRICE

Federal Recycling Program

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, DC 20555-0001

OFFICIAL BUSINESS