PNNL-13723

Pacific Northwest National Laboratory
Operated by Battelle for the U.S. Department of Energy

A Dictionary for Transparency

RT Kouzes

November 2001

Prepared for the U.S. Department of Energy
under Contract DE-AC06-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC06-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm


This document was printed on recycled paper.
(8/00)

PNNL- 13723

A Dictionary for Transparency

Richard Kouzes

November 16, 2001
July 6, 2002
December 24, 2002

Prepared for
The U. S. Defense Threat Reduction Agency

Pacific Northwest National Laboratory
Richland, Washington 99352

A Dictionary for Transparency

Richard Kouzes
Pacific Northwest National Laboratory
November 16, 2001 (Revised October 14, 2002)

Introduction

There are many terms that are used in association with the Defense Threat Reduction Agency (DTRA) Transparency Project. This is a collection of proposed definitions of some of these terms. There is a *Materials Protection Control and Accounting Glossary* with Russian translations (PNNL-11762) with a small overlap of information with this document. The International Atomic Energy Agency also has an out of print *Safeguards Glossary* of terms (IAEA/SG/INF/1 1987) that has no overlapping terms with this document.

A

Absolute Control Room is the room in the Mayak Fissile Material Storage Facility that will contain the US monitoring equipment.

Accepted Baseline is the complete set of software units accepted by agreement for a monitoring regime. It includes onsite authentication software as well as operational software used in the measurement instrument.

Analysis Enclosure (AE) is a major modular subsystem in a Recording Device. It contains a gamma analyzer, computational block, input and output data barriers, security watchdog, DC power supply, and tamper indicating devices.

Anonymous Purchase is a process whereby the true purchaser and the intended purpose are hidden from the supplier as a means of obtaining a trustworthy and uncorrupted component. This procedure may be used by the Host Party to procure uncorrupted components for use and by the Monitoring Party to procure a baseline copy for future comparisons during authentication activities. An Anonymous purchase assumes a mass market for the items, and is not possible when the market is less than many hundreds of items/year.

Applications Software is defined as software used to implement data analysis and equipment control. Equipment control software includes all the software used to support the basic functioning of the equipment used for measurements, as well as data collection from that equipment. For example, the Canberra Inspectors use drivers (from a support library), software to collect the data, and software to analyze the data. This is all applications software and subject to full disclosure of source code.

Applications Specialist for an instrument is the most knowledgeable person about that particular instrument available for consulting with monitors. Normally he/she will have been the task officer for the development or authentication of the equipment.

Attestation is the final step of information security certification (see). Information security certification consists of two elements: certification of individual hardware and software components and "attestation" of the integrated system of hardware, software, facilities and operating procedures. (Attestation is similar to system accreditation as practiced in the U.S. Government.)

Attribute is a specific physics related quantity derived from measurement and analysis. The four proposed attributes for material stored at Mayak are: presence of special nuclear material, weapons grade material, mass above a threshold, and presence of metal. The range of acceptable attribute values, as well as the algorithms for extracting attribute values from potentially classified data, can be openly discussed. An attribute-based measurement system contains some physics-based analysis to extract pre-agreed parameter values from the measurement data and generally uses statistical analysis for error propagation and result evaluation.

Attribute Measurement System (AMS) is measurement instrumentation that makes a measurement and analyzes the data to produce an attribute value. This term was also applied to the first specific system proposed for use in the FMSF absolute control room.

AT-400R (Atomic Transport 400 Russian) is a multi-layer stainless-steel container designed to hold fissile material at the FMSF. The current plan is that each AT-400R would hold about 4 kilograms of plutonium or 16 kilograms of HEU in the form of two balls held by an *insert*. For storage at the FMSF, each AT-400R is placed into a metal *basket*, and four such baskets are placed in a *shroud* for placement into a *nest*.

Audit and Examination (A&E) refers to a congressional mandate for inspections on all CTR programs for 3 years after completion to assure that equipment is in place and being used for its intended purpose.

Authentication is the process through which the Monitoring Party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item. (*Authentication Task Force definition*)

Authentication (IAEA) is the process of assuring that genuine information is obtained for safeguards purposes using equipment for which the IAEA lacks sufficient control or knowledge. (*IAEA definition draft May 2001*)

Authentication Assurance Level (AAL) is a package consisting of assurance components from document ISO/IEC 15408-3 that represents a point on the common criteria assurance scale that must be met to attain a given level of authentication

assurance. Each AAL represents a band of confidence obtained by requiring passage of selected documentation completeness levels and authentication measures. The AALs are most useful in balancing authentication requirements to avoid leaving a major credibility gap.

Authentication of Data is verification of the claimed identity of data provided by an active IT component (e.g., sensor, host computer). Authentication of Data is a cryptographic process used to verify that data originated from the specified source, was taken at the appropriate time, and has not been modified during transmission or storage. The process uses either digital signatures based on public/private key cryptography or message authentication codes based on symmetric key cryptography. This is often accomplished by creating a hash function of the data (such as a video frame), and securing it as an electronic signature using DES or public-key/private-key encryption.

Authentication Test Plan is defined as the detailed plan for the steps necessary to achieve authentication of the equipment. It is used to assure that the actual equipment system conforms to the provided documentation, functions only as specified, and meets the user requirements and the technical specifications.

B

Baseline is a set of critical observations or data used for comparison or control. Baseline implies a known, well-documented state. For example, baseline observations could be obtained from items either independently procured or obtained by random selection for extensive private examination. Authentication efforts in the field rely on comparisons to a set of baseline data. For example, installed software is compared to previously examined code.

Basket is a metal frame that holds one AT-400R Fissile Material Container. Four baskets are placed into a *shroud*, which is placed into a *nest*.

Black Box Testing is the term used to describe system testing performed in the absence of any information about the design of the system.

Buyer is the collection of government and private organizations representing the United States.

C

Calibration is the process of standardizing an instrument by determining the deviation from a standard so as to ascertain the proper scaling factors.

Central Processing Unit (CPU) is that portion of a digital computer, data-processing system, or device controller that executes the instructions contained in its program. The program and the data are usually stored separately from the CPU.

Certification (1) is the process by which a Host Party assures itself that an inspection system (which may be integrated with an information barrier) will not divulge any classified information about an inspected sensitive item to a Monitoring Party. Certification also includes all processes required for the Host to allow operation of the system within its facility. Certification in the Russian Federation needs to address both functional performance and information security. The first is required by both the Russian Law on Atomic Energy and the Law on Unity of Measurements. The second is required by Russian laws regarding the automated processing of "State Secrets." It is expected that functional certification will be carried out by the "OIT" system. This is a certification system jointly operated by Gosatomnadzor (GAN - Operator of Scientific and Technical Center on Nuclear and Radiation Safety), Minatom (Russian Ministry of Atomic Energy), and Gosstandart (set Russian standards) to certify "equipment, devices and technology" used in Russian nuclear facilities. There may be a related requirement to have certified measurement procedures developed by the Bochvar Institute. Information security certification falls under the authority of the Russian State Technical Commission (GOSTechKommisaya). Atominform (Minatom's information security testing center), Atomizaschitinform (Minatom's information security expert center), and Atomcertifika (Certification System Working Body managing day to day business of relevant certification system) also play a role in certification. The primary concern will be unauthorized disclosure of information. Certification considerations will affect both the individual components (hardware, software and firmware), and the integrated whole. The final step of information security certification is the so-called "attestation" when the entire system is reviewed and approved for use. (2) According to DOD 5200.40, the comprehensive evaluation of the technical and non-technical security features of an information processing system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of specified security requirements.

Challenge Measurements are defined operationally as a Monitor directed measurement with sources designed to address measurement integrity. Challenge measurements occur by definition only during normal operation. They are a simple method to quickly furnish some measure of confidence that the system is functioning properly. There are two major classes of challenge measurements:

- Type I: Measurements with known SNM sources that are designed to produce failure of a particular attribute. A low mass source, for example, would not pass a mass attribute.
- Type II: Re-measurements of containers that have passed previous inspection, but are measured again with an added source to produce a failure.

Closed Mode is one of two operating modes proposed for some measurement systems. (See also *Open Mode*.) Closed Mode (or secure mode) is the mode of operation of a measurement system in which both non-sensitive and sensitive items

may be measured. The measurement of non-sensitive items provides additional assurance to the monitors that the results from a system are accurately reflecting the items being measured in Closed Mode. In this mode, only binary measurement status, error, and attribute-result indications are displayed on the front panel of the closed, secure system enclosures. Closed Mode operations provide no method for obtaining or displaying intermediate results and/or measured values of the four attributes. In summary, Closed Mode operations prohibit the Host and the Monitoring Party from viewing or obtaining any sensitive material-attribute information.

Cobra Seal is a type of tamper indicating device using a fiber optic cable with photographic verification of tampering.

Commercial off the Shelf (COTS) is a commercial product that is available for anonymous purchase in a mass market.

Common Criteria are international standards that provide a common set of requirements for the security functions of information technology products and systems and for assurance measures applied to them during a security evaluation.

Common (Evaluation) Methodology is the methodology for authentication measurements evaluation; it describes the minimum actions to be performed by an evaluator to conduct a common-criteria evaluation.

Confidence is a faith, belief, or assurance that parties to an agreement will act in a right, proper, or effective way. In statistics, the reliance placed in a statement about a parameter, usually expressed as a probability that the statement is true.

C/FGI-MOD is Confidential Foreign Government Information Modified Handling Authorized, a subset of FGI (see). Foreign government documents either retain their original markings (confidential, secret, top secret) or are otherwise marked C/FGI-MOD. C/FGI-MOD documents shall only be shared with persons with a demonstrable need to know.

Container, or *fissile material container*, is an AT-400R designed to hold fissile material in the FMSF.

Containment and Surveillance (C/S) is the process of monitoring material or equipment to ensure that it cannot be removed or tampered with without detection.

Continuity of Knowledge (CoK) is the continuous knowledge of the location and state of material or equipment. For equipment or material under C/S, CoK is maintained if there is no break in surveillance coverage and/or the tamper indicating enclosure and tamper indicating device show no evidence of tampering.

Continuity of Knowledge (CoK): For purposes of the FMS, CoK of material is defined as "knowing the identification and location of every AT-400R container at all times following declaration."

Continuity of Knowledge Assurance Level (CoKAL): A concept proposed by PNNL analogous to the Authentication Assurance Levels (see), CoKALs can be defined that measures the level of CoK for a specific item. Each increasing CoKAL assumes the previous level of CoKAL coverage.

Cooperative Threat Reduction (CTR) program of the U.S. Department of Defense is designed to help the countries of the former Soviet Union destroy nuclear, chemical, and biological weapons of mass destruction and associated infrastructure, and to protect against the proliferation of those weapons.

D

Declaration means a formal document giving explicit details in compliance with an agreement. In the case of the FMSF, the Russian Federation will provide to the US Monitors a declaration about the identities and contents of containers stored in the massif.

Defect means a difference between the declared amount of nuclear or non-nuclear material and the actual amount present. A defect could involve any fraction of the declared amount, which could be an overstatement or an understatement of the amount measured. (IAEA definition)

Defect means a condition of an item that does not meet the expected characteristics. For the Mayak FMSF, this is the failure of a container to meet at least one required material attribute, or a missing container.

Defective Item is defined as a container that fails to meet one or more of the prescribed attribute criteria.

Defense Threat Reduction Agency (DTRA) is the implementing agency for the U.S. Department of Defense Cooperative Threat Reduction Program. It has four functions: combat support, technology development, threat control, and threat reduction.

Department of Energy (DOE) is the agency responsible for fostering a secure and reliable energy system, for stewardship of the Nation's nuclear weapons, for facility cleanup, and for supporting continued leadership in science and technology.

Design Validation- The determination of completeness and correctness of the hardware design based upon requirements documentation.

Design Verification- The demonstration of consistency, completeness, and correctness of the hardware design based on requirements.

E

Eddy-Current Testing: A technology that can be used to verify the integrity of a container and identify the signature associated with certain container features, such as a weld.

EM-coil: A technology using an induction coil around an item and low frequency electromagnetic waves (about 10 Hz – 1000 Hz) to measure the complex impedance response of the item. The data produced at a single frequency, or a range of frequencies, provides a template comparison between items that is unique to a given conductor configuration.

Enrichment refers to the percentage of ^{235}U in a uranium item. HEU is material with greater than 20% ^{235}U.

Evaluation Assurance Level (EAL) is a package consisting of assurance components from document ISO/IEC 15408-3 that represents a point on the common criteria assurance scale that must be met to attain a given level of security assurance.

F

Factory Acceptance Test (FAT) is performed at the fabrication and integration facility prior to shipment of equipment to the facility.

Facility Monitoring System (FMS) is a system of control and containment for providing U.S. CoK in the FMSF. A specific FMS system implementation consisting of video, portal and area radiation monitors, and TIDs for the FMSF was specified by LANL.

False Negative is a measured negative result for an item that actually has the declared attribute.

False Positive is a measured positive result for an item that actually does not have the declared attribute.

Fissile Material Container (FMC) is an AT-400R container holding fissile material in the FMSF.

Fissile Material Storage Facility (FMSF) is the storage building complex at Mayak that is being built with U.S. funds by Russian contractors to store weapon-origin material in a safe and secure manner to prevent any military reuse.

Flaw is an inadvertent or intentional condition or action of a *System* that can or does cause incorrect output.

For Official Use Only (FOUO) is a DOD designation of sensitive unclassified information similar to OUO (see) that may be exempt from release under the Freedom of Information Act. Access must be restricted to government and/or contractor staff with a valid need to know. It has government statute backing, unlike OUO.

Foreign Government Information (FGI) is 1) information provided to the U.S. Government by a foreign government or governments, an international organization of government, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence; 2) information produced by the U.S. pursuant to or as a result of a joint arrangement with a foreign government or governments, or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence; 3) information received and treated as "FGI" under the terms of a predecessor order.

Functional Testing is testing of systems and components to ensure that they function as designed and disclosed. Functional testing of radiation monitoring equipment includes, but is not limited to, testing with a set of physical and/or electronic sources.

G

Gamma Ray Detector is a device for measuring gamma radiation. Typically a NaI detector or a HPGe detector.

Golden Copy refers to a copy of a hardware or software component that is trusted to be authentic by its owner. It is used for comparison purposes during inspections to ensure that items have not been modified.

Grey Box Testing is a term used to describe system testing performed using partial information about the design of the system.

H

Hash Function: A hash function is a cryptographic function used to produce a fixed-length output string from an arbitrary-length input. It is a one-way function, meaning that it is easy to calculate the output for a given input, but it is virtually impossible to find an input that will give a specified output. Hash functions can be used in data

authentication and software integrity verification protocols. (See Software Integrity Verification.)

Hidden Switch refers to a covert means, in either software or hardware, to alter the outcome of a monitoring measurement. A flaw that allows the equipment to pass calibration and testing activities conducted by the monitoring party and then change to a mode that allows prohibited items to be accepted as allowable. Some of the ways in which the hidden switch can be activated include operator intervention, radiation or sound applied externally to the equipment, and the characteristics of the item being measured.

Highly Enriched Uranium (HEU) is uranium containing more than 20% of the isotope uranium-235.

High-Purity Germanium Detector (HPGe) is a gamma-ray detector based on a high purity germanium crystal. An HPGe may be stored at room temperature when not in use.

High-Resolution Gamma Spectrometry (HRGS) distinguishes between gamma rays of very similar energies. In modern times, it is usually achieved with germanium detectors.

Host Party refers to the country or representatives of the country that owns the facility being monitored; the Russian Federation or its representatives for the Mayak FMSF regime.

Host Supply of equipment implies that the Host Party will provide all measurement and surveillance systems. At a minimum, Host-supply means that the Host has last private access to all the equipment to perform certification. Under Host-supply, the Host may obtain portions of the hardware and/or software from vendors associated with the Monitoring Party.

I

Information Barrier (IB) consists of technology and procedures that prevent the release of Host-Country classified information to a Monitoring Party during a joint inspection of a sensitive item, while promoting assurance of an accurate assessment of Host Country declarations regarding the item.

Insert is the assembly that fits inside an AT-400R container and holds the two spheres of plutonium or HEU.

Integrated Control System (ICS) is the system that controls and monitors the the infrastructure, MPC&A, and security systems at the FMSF.

Integration is the process of combining sub-systems of detectors, hardware, and software into operational systems with all the documentation, functional testing, and procedures necessary for the regime.

Information Technology (IT) encompasses all technology used to create, store, exchange, and use information such as data, conversations, images, multimedia, and other forms. It covers both telephony and computer technology.

International Atomic Energy Agency (IAEA) is an independent intergovernmental, science and technology-based organization in the United Nations family. It assists member states with nuclear technology issues, and verifies through its inspection system that States comply with their commitments under the Non-Proliferation Treaty and other non-proliferation agreements, to use nuclear material and facilities only for peaceful purposes.

Inventory is the list of items contained in the FMSF, or a periodic inspection of some sample of stored items conducted by the Host party.

Inventory Sampling Measurement System (ISMS) is the specific monitoring system to be used in the FMSF absolute control room to measure agreed attributes of stored material selected by the sampling plan during monitor visits. The ISMS is specified by the US, and designed, integrated, installed and operated by the RF under direction of US Monitors.

Isotopic Ratio, in reference to a plutonium item, is the ratio of the amount (number of atoms) of ^{240}Pu to ^{239}Pu.

J

Joint Executive Committee (JEC) is a U.S.-R.F. group that manages the implementation of the monitoring regime at FMSF Mayak.

Joint Experts Visit (JEV) is an initial monitoring visit at FMSF Mayak by technical experts from both the US and the RF.

K

L

Low Intrusion Technology is a term used to describe monitoring technologies that inherently do not reveal detailed or possibly classified information about an item. Examples of low intrusion technology include the EM-coil, thermal imaging, and ultrasonic imaging.

M

Massif refers to room 401 of the FMSF which contains the nests where plutonium and HEU items will be stored.

May, as a verb used in a functional specification or statement of work, indicates a desirable feature that observes "best practices" but is not imperative

Mayak is the RF site which once produced plutonium for weapons and is the location of the Fissile Material Storage Facility.

Mean Time to Failure is the mean operating time accumulated by a device or system before a failure causes the device or system not to be able to perform its function.

Monitor is a member of the US team that will visit the FMSF to perform monitoring measurements and observations.

Monitoring Party is the country or organization that is monitoring a facility. The term generally refers to the United States or its representatives when related to a bilateral FMSF regime. It is also recognized that the International Atomic Energy Agency could act independently as the Monitoring Party under another regime.

Monitoring System is an instrument used to measure attributes or templates for a monitor in a monitoring regime.

Monitoring Visit is one of the planned visits by US monitors to the FMSF, proposed to be six times per year.

Multichannel Analyzer (MCA) is an instrument that measures the height of electrical pulses presented to it and builds a histogram containing the distribution of pulse heights. An MCA is an essential component of almost every gamma-ray spectrometer. The histograms often represent gamma-ray energies corresponding to the type of radioactive material in a source.

N

Nest is one of the 3168 tubes in the massif at FMSF that will hold plutonium and/or HEU. A nest can hold two shrouds, each with up to four containers in baskets. The term *silo* is also used by the RF for this structure.

Nest Cover is the lid that covers and seals a nest in the massif.

Neutron Multiplicity Counter (NMC) is an instrument that determines the frequencies with which different numbers of neutrons (2, 3, 4, etc.) are emitted simultaneously by a source. Plutonium-240, present in weapons-grade plutonium, fissions spontaneously emitting a few neutrons with every fission. These multi-neutron events may be quantified with the aid of an NMC to produce an effective mass.

O

Official Use Only (OUO) is a designation of sensitive unclassified information that may be exempt from release under the Freedom of Information Act. OUO must meet the "two test" criteria. Access must be restricted to government and/or contractor staff with a valid need to know. Foreign government information is not one of the category exemptions specified in OUO. FOUO (see) has government statute backing, unlike OUO.

Open Mode is one of two operating modes proposed for some measurement systems. (See also *Closed Mode***.**) Open Mode operations is the mode of operation of a measurement system in which only non-sensitive background, calibration, or reference sources will be measured. The goal of such measurements is to provide assurance that the systems operate accurately. In Open Mode, attribute measurements are performed with open enclosures, allowing Host and Monitoring Parties to observe information on the diagnostic video displays, showing information such as the full gamma-ray spectrum and intermediate physics-analysis results.

P

Passport is a template that characterizes an item in the FMSF. The passport is generated by one of the five Passport Systems used by the RF in room 357 of the FMSF.

Passport System is a template measurement system that characterizes an item in the FMSF through a measurement of gamma and neutron radiation. The passport system generates a passport for an item that enters the FMSF. There are five passport stations to be used by the RF in the FMSF.

Photographic Comparison is the acquisition and analysis of archival images for applications related to knowledge of an item or component, relying on intrinsic features of the item.

Physical Protection is the application of physical, technical, and administrative methods designed to: protect personnel; prevent or detect unauthorized access to facilities, material, and documents; protect material against espionage, sabotage, damage, and theft; and respond to any such acts as they occur.

Physical Protection Equipment is a generic term encompassing any item, device, or system that is used primarily for the protection of property and resources, personnel, installations, and facilities.

Plenum is the area underneath the nests in the massif of the FMSF that is used for air handling for cooling of the stored material.

Portal Monitor is an electronic instrument designed to perform scans of items, personnel, and vehicles entering or leaving a designated area for the purpose of detecting weapons, explosives, or nuclear material.

Procedures are written descriptions of the steps involved in performing specific operations, which could include design practices, manufacturing processes, authentication activities, or inspection protocols.

Public/Private Key refers to a class of cryptographic functions that use different keys for different operations. One key is usually made public, while the other is kept secret. For data authentication, the secret key is used to sign the data, and the public key is used to verify the signature. Also referred to as "public key" or "asymmetric" cryptography.

Q

R

Random Access Memory (RAM) is computer memory whose individual storage locations, or addresses, may be written to or read from with nearly equal ease at almost any time. This is distinct from storage on tape, a disk, or some other media, where mechanical motion makes only certain addresses available at a given time.

Random Selection refers to the process by which the Monitoring Party selects among a group of duplicate Host-supplied components that have been fully tested and certified for (1) installation into inspection equipment and (2) private examination. After random selection, both parties jointly hold the installed component/system under some combination of tags, seals, and video surveillance to preclude any unauthorized modifications. Random selection is beneficially applied at installation to complete systems or during subsequent visits to components, spare parts, or subsystems.

Recording Device (RD) was the proposed attribute measurement system to be located in the FMSF in association with the RF Passport Systems.

Regime is an established system or way of doing things.

Reliability is the continued ability of a component to complete its intended function with independent confirmation of that ability.

Reloader is the device used in the massif of the FMSF to move shrouds containing items between the hatch in the assembly room and the nests.

Remote Monitoring System is an unattended monitoring system that electronically communicates monitoring data to monitors at another site.

Russian Party refers to the Russian Federation or its representatives for the Mayak Storage Facility regime.

Russian Supply of equipment implies that the Russian Party will provide all measurement and surveillance systems. At a minimum, Russian-supply means that the Russian Party has last private access to all the equipment to perform certification. Under Russian-supply, the Russian Party may obtain portions of the hardware and/or software from vendors associated with the U.S. Party. (This definition is a specific example of Host Supply)

S

Safeguard is any technique or procedure or other measure that reduces Vulnerability.

Sampling Plan is a statistical means used to select a portion of items for measurement or other special attention.

Seals are physical devices that provide permanent evidence of any attempt to gain access to a sealed item.

Secure Mode (or closed mode) is the mode where both non-sensitive and sensitive items may be measured. The measurement of non-sensitive items provides additional assurance to the monitors that the results from a system are accurately reflecting the items being measured in Closed Mode. In this mode, only binary measurement status, error, and attribute-result indications are displayed on the front panel of the closed, secure system enclosures. Closed Mode operations provide no method for obtaining or displaying intermediate results and/or measured values of the four attributes. In summary, Closed Mode operations prohibit the Host and the Monitoring Party from viewing or obtaining any sensitive material-attribute information.

Secure Storage is a requirement imposed on the FMSF to provide safe and secure storage of items of plutonium and/or HEU.

Secure Storage System is a term specifically applied to the TIDs and related procedures for providing confidence in the secure storage of material at the FMSF.

Security Watchdog monitors and maintains monitoring system security.

Shall, as a verb used in a functional specification or statement of work, indicates a firm requirement.

Shroud is a metal frame that holds up to four baskets of containers, and which is placed into a nest. A nest can hold two shrouds.

Silo is one of the 3168 tubes in the massif at FMSF that will hold plutonium and/or

HEU. The term *nest* is also used by the US for this structure.

Site Acceptance Test (SAT) is a test performed at the installation site (FMSF) to demonstrate full operability and compliance with specifications.

Software Design Validation is the determination of completeness and correctness of software based upon requirements documentation.

Software Design Verification is the demonstration of consistency, completeness, and correctness of software based on requirements.

Software Integrity Verification is a cryptographic protocol that can be used to verify that an unaltered copy of a set of software and/or firmware exists on a system. The protocol uses a hash function and a secret key to compare the software/firmware on an untrusted computer system to a certified copy on a trusted computer system.

Source refers to a radioactive item that is usually used for the calibration of a monitoring system.

Spare is one of the replacement subsystems of components of a monitoring system. Spares will be used for both the repair of systems, and for the purpose of random selection for authentication.

Special Nuclear Material (SNM) in this context refers to plutonium or HEU.

Spoof is an attempt to pass a false item in place of a real item.

Symmetric Key refers to a set of cryptographic functions and protocols that use the same key for both encryption and decryption (or signing and verifying) the data. Also referred to as “private key” cryptography.

System is the complete ensemble of software and hardware.

System Effectiveness is the measure of the ability of a system to detect a defect.

T

Tag is a strip of paper, metal, or plastic hung from or attached to an item to identify, classify, or label the item.

Tamper-Indicating Device (TID) is a device or seal that provides permanent evidence of any attempt to gain access to the sealed item. Each TID must be uniquely identifiable to preclude replacement with a counterfeit duplicate.

Tamper-Indicating Enclosure (TIE) is an enclosure with tamper indicating features that provides permanent evidence of any attempt to gain entry to the interior. The

enclosure can either be self-sealing or sealed with an external Tamper-Indicating Device.

Template Measurement System is a term applied to a measurement system that makes a comparison of measurements, such as parts of gamma ray spectra, between an unknown item and a known item. A template-based system may just state that the two items are similar or different using statistical comparison techniques without necessarily using any physics-based data analysis to extract fundamental attribute values.

Testing is a formal process of inspection or execution of the system intended to disclose Flaws or reveal ways in which the system fails to meet its requirements.

Third Party Software is non-commercial software used in the accepted baseline developed by neither the host nor the monitoring party.

Threat is a circumstance or event that could lead to the creation and/or exploitation of a Flaw in the System. The degree of threat is simply the potential for exploiting a Vulnerability.

Transparency is a method for gaining confidence by examination and provision of objective evidence that specified requirements have been fulfilled. *Transparency* is often used as a term to mean that the design and operations of a monitoring system are completely open and understood by all parties. (see Verification)

Transparency Regime refers to a regime where there is a desire to perform some specified action in an open manner so that all parties gain confidence that the specified action has occurred. A Transparency Regime requires less confidence by direct inspection/measurement than a Verification Regime where the national security stake is higher. (see Verification Regime)

Transparent System refers to a completely documented system where one has the ability to look in all the design and component details as a means of gaining a full understanding of all the processing occurring within the system. (see Verification)

U

UCNI is unclassified government information whose unauthorized dissemination is prohibited under Section 148 of the Atomic Energy Act of 1954, as amended, and DOE Order 471.1

Unattended Monitoring System: A monitoring system designed to take data on the operation of the facility being monitored while the representative of the monitoring party are not present.

Unique Identification Code (UIC) of an AT-400R container consists of its barcode, container identification number, and weight.

Unique Identifier is any device or feature that is used to uniquely identify an item. A secure unique identifier is such an identifier that cannot be counterfeited or transferred from an authenticated item to one that has not passed the authentication procedures.

United States (U.S.): The United States of America; the abbreviation is used when the term is an adjective, and the term is written out when it stands alone.

V

Variable Coding Sealing System (VACOSS) is an example of an active fiber-optic seal. VACOSS seals are composed of three major components: the seal body, the fiber-optic cable, and the readout cable.

Validation is confirmation by examination and provision to obtain objective evidence that the particular requirements for a specific intended use are fulfilled.

Validation (Materials Protection Control and Accounting) is

- Confirmation, by testing, that an implemented, operational system or critical system element meets established requirements.
- Process used to verify the accuracy of data gathered during an inspection or survey.

Verification is confirmation by examination and provision to obtain objective evidence that specified requirements have been fulfilled. (see Transparency)

Verification (Materials Protection Control and Accounting): Process whereby information is evaluated relative to appropriate standards.

Verification is confirmation that an item is in agreement with the operator's declaration. (IAEA)

Verification Regime refers to an agreement to perform some specified action and allow the other parties to the agreement to ensure that the specified action has occurred. A Verification Regime generally applies when national security is at risk if the action is not performed as agreed. A Verification Regime requires a higher degree of confidence regarding compliance than a Transparency Regime. Many of the methods of achieving sufficient confidence are similar, but they are pursued more vigorously and with more resources. (see Transparency Regime)

Vulnerability (Physical Protection): Exploitable weakness or deficiency in a system or at a facility. A weakness in design or implementation that could be exploited to create Flaws and/or compromise classified information.

Vulnerability Assessment/Analysis (VA) (PP): Systematic evaluation process in which qualitative and/or quantitative techniques are used to identify vulnerabilities and recommend upgrades to a Materials Protection Control and Accounting system.

Vulnerability Assessment (Host) is the set of procedures typically used by the Host Party to identify potential security threats to a system. It would establish that the procedures for, and the design of, an information-barrier-protected system adequately protect classified information over the entire lifecycle of use. The Host's assessment would include consideration of potential methods of covertly extracting information and the probability of discovering all such methods. (see Certification)

Vulnerability Assessment (Monitor) is the set of procedures typically used by the Monitoring Party to identify potential threats to a system relative to the credibility of an information-barrier-protected system (authentication) and to establish that authentication efforts are adequate relative to the regime. A Monitoring-Party vulnerability assessment would consider the probability of the authentication team finding various example spoofs/hidden switches and the completeness of the authentication effort.

Vulnerability Assessment Level (VAL) is a package consisting of assurance components from document ISO/IEC 15408-3 that represents a point on the common criteria assurance scale that must be met to attain a given level of authentication assurance. The VALs have been defined by the IAEA for their evaluation of monitoring equipment.

W

Weapons Grade refers to an item of plutonium that could be utilized for a nuclear weapon based upon having an isotopic composition consistent with that purpose. Weapons grade usually refers to material with an isotopic ratio of ^{240}Pu to ^{239}Pu of about 6%. For the purpose of Mayak transparency, weapons grade Pu is defined as material having an isotopic ratio of less than 0.1.

Weapons Origin implies the fact that material has come from the disassembly of a nuclear weapon.

Will, as a verb used in a functional specification or statement of work, indicates a highly desirable feature that software or hardware should have.

With Replacement is a term used in the statistical sampling plan sense meaning that once an item is sampled under the sampling plan, the item is placed back in the population and may be sampled again in the future.

Without Replacement is a term used in the statistical sampling plan sense meaning that once an item is sampled under the sampling plan, it is not placed back into the

population for later sampling. That is, once measured, an item is not ever re-measured again.

X

Y

Z

Zero Defect Sampling is used in the context of the sampling plan to mean that if containers are sampled, and if no defects are found in the sample set (i.e. zero defects), then a statistical conclusion can be drawn as to the probability of defects existing in the total population. Thus, obtaining a sample of 300 containers out of a population of 12,000 containers, and finding zero defects, provides a 95% confidence level that fewer than 1% defects exist in the population.

Acronyms

AAL	Authentication Assurance Level
AMS	Attribute Measurement System
BIOS	Basic Input/Output System
CFGIMOD	Confidential Foreign Government Information Modified Handling Required
CoK	Continuity of Knowledge
CoKALs	CoK Assurance Levels
COTS	Commercial off the shelf
CPU	Central Processing Unit
CTR	Cooperative Threat Reduction
DOE	U.S. Department of Energy
DoD	U.S. Department of Defense
DTRA	U.S. Defense Threat Reduction Agency
EAL	Evaluation Assurance Level
EMI	Electromagnetic Interference
FAT	Factory Acceptance Test
FGI	Foreign Government information
FIPS	Federal Information Processing Standards
FMC	Fissile Material Container
FMCP	Fissile Material Control Program
FMS	Facility Monitoring System
FMSF	Fissile Material Storage Facility
FOUO	For Official Use Only
HEU	Highly Enriched Uranium
HPGe	High-Purity Germanium Detector
HRGS	High-Resolution Gamma Spectrometry
IAEA	International Atomic Energy Agency
IB	Information Barrier
IBWG	Information Barriers Working Group
IC	Integrated Circuit

ICS	Integrated Control System
ISMS	Inventory Sampling Measurement System
ISO	International Standards Organization
IT	Information Technology
JEC	Joint Executive Committee
JEV	Joint Experts Visit
JTAG	Joint Technical Advisory Group
Mayak PO	Operator of Ozersk site responsible for overall operation of FMSF
MCA	Multichannel Analyzer
NIST	U.S. National Institute of Standards and Technology
NMC	Neutron Multiplicity Counter
NSA	National Security Agency
OUO	Official Use Only
PP	Physical Protection
RAM	random access memory
RD	Recording Device
R.F.	Russian Federation
RF	Radio Frequency
RFI	Request for Information
RFP	Request for Proposals
SAT	Site Acceptance Test
SNM	Special Nuclear Material (usually plutonium or HEU)
STIE	Secure Tamper-Indicating Enclosure
TID	Tamper-Indicating Device
TIE	Tamper-Indicating Enclosure
TOE	Target of Evaluation
TSOW	Technical Statement of Work
UCNI	Unclassified Government Information
UIC	Unique Identification Code

VNIIEF	All-Russian Scientific Research Institute of Experimental Physics in Sarov (Arzamas-16)
VNIITF	All-Russian Scientific Research Institute of Theoretical Physics in Snezhinsk (Chelyabinsk-70)
VNIPIET	All-Russian Design and Scientific Research Institute of Complex Power Technology
WG	Weapons Grade