PNNL-13637

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

Authentication Assurance Level Application to the Inventory Sampling Measurement System

Version 1.0

M.M. DeVaney
R.T. Kouzes
R.R. Hansen
B.D. Geelhood

August 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-13637

Authentication Assurance Level
Application to the Inventory Sampling Measurement System[1]

Version 1.0

29 August 2001

M. DeVaney, R. Kouzes, R. Hansen, and B. Geelhood

Prepared for
The U. S. Defense Threat Reduction Agency

Pacific Northwest National Laboratory
Richland, Washington 99352

[1] This paper is one of four documents developed by PNNL that introduce the application of the CC to authentication:
Authentication Assurance Levels: A Strategy for Applying The ISO Common Criteria Standards
Authentication Assurance Level Application to the Attribute Measurement System
A Review of the IAEA Vulnerability Assessment Level Scheme: Applicability to DTRA and DOE Programs in the FSU
Inventory Sampling Measurement System (ISMS) Common Criteria Authentication Protection Profile (ISMS-A-PP)

TABLE OF CONTENTS

1 INTRODUCTION

A major mission of the United States Defense Threat Reduction Agency (DTRA) is to monitor compliance in the states of the Former Soviet Union (FSU) under the Non-Proliferation Treaty and other non-proliferation agreements. FSU countries are dismantling nuclear weapons and storing the associated weapons origin Plutonium in potentially monitored facilities (e.g., the Fissile Material Storage Facility (FMSF) at Mayak, Russia). The DTRA has recognized the need for effective verification of non-proliferation undertakings monitoring of weapons origin nuclear material and activities.

The attainment of DTRA's goal of assuring nuclear non-proliferation compliance in the FSU will rely on the establishment of an integrated monitoring system which uses a sound conceptual and technical framework, employing modern and internationally accepted techniques, to facilitate the deployment of new technologies to strengthen systems (e.g. to provide improved surveillance techniques, remote monitoring and environmental sampling).

Two of the essential techniques needed by such a framework are standardized approaches for the 1) specification of Information Technology security functions, and 2) a standardized assessment approach to verify the implementation of such required functions in the equipment to be deployed.

This document concentrates on the identification of a standardized assessment approach for the verification of security functionality in specific equipment, the Inventory Sampling Measurement System (ISMS) being developed for Mayak. [Kouzes2001a] Specifically, an Authentication Assurance Level 3 (AAL3) is proposed to be reached in authenticating the ISMS. [Kouzes2001b]

A standardized approach for the specification of security functions is outside the primary scope of this document, although ISO/IEC 14508, Common Criteria for Information Technology Security Evaluation [CC], which is referenced extensively in this document, addresses both the specification of security functions and the assessment of their implementation. The Common Criteria has been adopted by 14 countries including the United States. In the FSU, the Russian Federation (RF) is undertaking to adopt the Common Criteria.

1.1 Objective

The primary objective of this paper is to define information technology (IT) security evaluation criteria for the Mayak ISMS equipment system and application software that are based on internationally accepted criteria and are appropriate and effective for re-use in subsequent nuclear non-proliferation compliance monitoring equipment systems. This calls for the definition of appropriate and effective methodologies and procedures for specifying and authenticating the functionality of monitoring equipment. It should define sets of criteria that DTRA and the RF can jointly use in contracting for systems.

A secondary objective of this document is to identify any supplementary activities recommended to fully implement the evaluation criteria.

This document outlines the appropriate and effective methodology and procedures for specifying and authenticating security targets for nuclear non-proliferation compliance monitoring equipment systems. As such, it considers all parties involved in the assessment and operation of the equipment: the developers of the technology, the assessors performing authentication analysis on the technology, and the users of the technology in the operational environment.

1.2 Terms and Definitions

Authentication: The process through which the Monitoring party gains appropriate assurance that the information reported by a measuring system accurately reflects the true state of the monitored item. Thus, authentication focuses on the credibility of the result rather than the confidentiality of classified information. [Kouzes2001c]

Authentication Assurance Level: One of a set of assurance packages (defined in this document) consisting of assurance components from [CC3] that represents a point on the [CC] assurance scale...that must be met to attain a given level of security assurance.

Common Criteria: Common Criteria for Information Technology Security Evaluation, see [CC].

Common (Evaluation) Methodology: Common Methodology for Information Technology Security Evaluation describes the minimum actions to be performed by an evaluator in order to conduct [CC] evaluation, see [CEM].

Evaluation Assurance Level: From [CC1], a package consisting of assurance components from [CC3] that represents a point on the [CC] assurance scale (...that must be met to attain a given level of security assurance).

Protection Profile: From [CC1], an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific user needs. It captures the required security functionality and security assurance requirements, along with the threats addressed and the environments in which the compliant product would apply.

Security Critical Component: A software or hardware component essential to the security function of the equipment. Any changes to a Security Critical Component must be evaluated to ensure that the security functionality of the system has not been compromised.

Security Target: From [CC1], a set of security requirements and specifications to be used as the basis for the evaluation of an identified TOE.

Target of Evaluation: From [CC1], an IT product or system and its associated administrator and user guidance documentation that is the subject of (security) evaluation.

Vulnerability assessment: From [CC3], the identification of exploitable vulnerabilities introduced due to the construction, operation, misuse, or incorrect configuration of the corresponding system or software.

1.3 Acronyms

AAL	Authentication Assurance Level
CC	Common Criteria for IT Security Evaluation (see [CC])
CCRA	Common Criteria Recognition Arrangement
CEM	Common Methodology for IT Security Evaluation (see [CEM])
COTS	Commercial off the shelf
DTRA	Defense Threat Reduction Agency
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IEC	International Electrotechnical Commission
ISMS	Inventory Sampling Measurement System
ISO	International Organization for Standardization
IT	Information Technology
OR	Observation Report

PNNL	Pacific Northwest National Laboratory
PP	Protection Profile
ST	Security Target
TOA	Target of Authentication
TOE	Target of Evaluation
TSF	TOE Security Functions

2 BACKGROUND

2.1 Automated Measurement System at Mayak

The Defense Threat Reduction Agency (DTRA) is funding the construction of the Fissile Material Storage Facility (FMSF) at Mayak to facilitate Russian storage of thousands of canisters containing weapon-origin plutonium and possibly highly enriched uranium. The US has funded the FMSF with the conditions that the facility will provide: 1) storage of weapons-origin material, 2) safe and secure storage of this material, and 3) no re-use of this material for military purposes. The non-proliferation goal is to prevent diversion of this fissile material into any future nuclear weapon program (Russian Federation or other country).

DTRA is funding the Russian Federation development of two measurement systems protected by an information-barrier (IB) for use at FMSF. The Recording Device (RD) is proposed to observe each canister entering FMSF and provide confidence that each contains plutonium with isotopics consistent with weapon-grade plutonium. The Inventory Sampling Measurement System (ISMS) is proposed to measure a statistical sampling of canisters from storage to provide confidence that each sampled canister is consistent with the declared mass of plutonium in metallic form with weapon-grade isotopics. DTRA is also funding development of a facility monitoring system (FMS) that uses these two measurement systems to initialize item accountability along with other approaches (e.g., tags and seals, video surveillance, radiation sensors, records, and data processing) to maintain continuity of knowledge (CoK) regarding item accountability of canisters containing special nuclear material. It is reasonable to assume that the FMS may include IB aspects because security measures are often considered classified and be subject to IB-related threats. The large effort to develop these measurement and tracking capabilities implies a requirement for credibility regarding the results. These three US-specified systems are largely intended to assure the US that the Russian operators of the facility are complying with the agreement. A separate and independent Russian physical-protection system consisting of domestic safeguards, surveillance and tracking measures, Passport radiation sensors, access controls, security alarms, and armed guards has primary responsibility for preventing theft.

These IB-protected systems will make non-intrusive radiation measurements on sealed canisters to determine whether the contents are consistent with the Russian declarations. The Russian Federation considers the isotopic composition of the material to be classified and will conduct a separate certification process to protect the confidentiality of that information. The Russian Federation Host therefore is allowed to supply the IB-protected measurement systems to fully ensure that the Host's declared classified information is provided paramount protection during the measurements, analysis, and comparison with pre-agreed criteria. Although the US never sees any classified data, the US must have confidence that displayed results accurately indicate satisfaction of all the pre-agreed criteria. The IB system design is assumed to be fully transparent, i.e. its operation is completely understood in detail by the US. The US's authentication process is not directly concerned with protecting classified information, but must respect legitimate system-access limitations required to protect classified information.

The RD has the most *a priori* vulnerabilities: daily operation by Russians, and total Russian control of the canister input stream. However, the RD will be routinely independently validated by subsequent ISMS measurements on a statistical sampling of canisters.

Authentication is the process through which the Monitoring party gains appropriate assurance that the information reported by a measuring system accurately reflects the true state of the monitored item. Thus, authentication focuses on the credibility of the result rather than the confidentiality of classified information.

2.2 Common Criteria

This document uses the Common Criteria for Information Technology Security Evaluation ("Common Criteria", or "CC"), (ISO/IEC 15408), as a tool for developing the authentication assurance evaluation criteria prescribed. Although the CC addresses both functional requirements and assurance requirements, this document concentrates on the definition of assurance requirements.

The CC is a catalog of criteria and a framework for organizing a subset of the criteria into security specifications. The CC is also a set of tools that allow for the construction of IT security requirements. The CC strictly addresses the functional and assurance requirements for IT security. Administrative measures not directly related to IT security are outside the scope of the CC. Using the CC as a standard permits independent evaluations to be compared. The CC does this by providing a "common" set of requirements for security properties of IT products and a "common" set of assurance measures that can be applied to those products during an evaluation. These requirements serve as guides for the development of IT products, the procurement of products with IT security features, and are a basis for evaluation of IT security products.

2.3 CC Framework

Figure 1 provides a high level view of the CC framework. For our purposes the acronym TOE (Target of Evaluation) is the ISMS in its entirety (formally the CC defines the TOE as the security related part of the system undergoing evaluation). Threats identified in the security environment lead to the development of security objectives, which are in turn satisfied by selecting appropriate security requirements from the catalogs in [CC2] (functional) and [CC3] (assurance). The developer of the system is responsible for implementing the requirements and presenting the system (TOE) for evaluation. The rationales (back pointing arrows) in Figure 1 indicate the tractability provided by the CC approach. An unsatisfied requirement can be traced back to the threat(s) less mitigated. A change in the security environment (change in threats, assumptions, or policies) can be traced forward to identify the security requirements that may require modification.

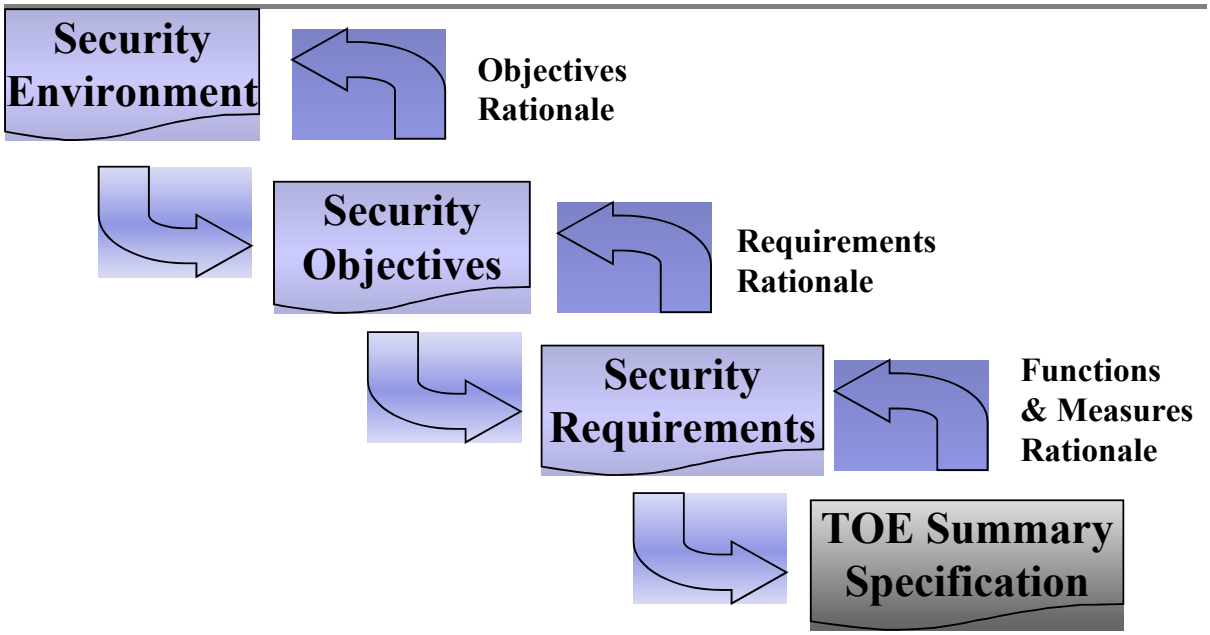

Figure 1: The Common Criteria Specification Framework

2.4 Common Criteria Functional Requirements Catalog

A catalog of functional security requirements criteria are available in [CC2] and are grouped in the following classes:

Security Audit (FAU)
Communication (FCO)
Cryptographic Support (FCS)
User Data Protection (FDP)
Identification & Authentication (FIA)
Security Management (FMT)
Privacy (FPR)
Protection of the TOE Security Functions (FPT)
Resource Utilization (FRU)
TOE Access (FTA)
Trusted Path/Channels (FTP).

Separately, Pacific Northwest National Laboratory (PNNL) is defining the functional requirements for authentication of the ISMS.

2.5 Common Criteria Assurance Requirements Catalog

A catalog of assurance security requirements criteria are available in [CC3] and are grouped in the following classes:

Configuration Management (ACM)
Delivery and Operation (ADO)
Development Documentation (ADV)
Guidance Documents (AGD)
Life-Cycle Support (ALC)

Testing (ATE)
Vulnerability Assessment (AVA)
Assurance Maintenance (AMA)

The eighth class, Assurance Maintenance, is often omitted from the list. Traditionally, evaluators focused on qualifying a system for initial use and required significant re-assessment activities to validate a modified system. This created a situation in which software validated under schemes predating the CC was rarely updated, making maintenance and modernization a nightmare. While the CC is addressing this issue, the effort generally lags the progress made in other areas. While the maintenance of confidence in ISMS results is critically important to DTRA, it has been determined that modification to the system will require re-authentication. Thus, there are no ISMS assurance requirements in the Assurance Maintenance class.

3 GENERAL REQUIREMENTS

3.1 Assurance Requirements

The focus of this document is to define the means by which the DTRA may gain confidence in the security properties of the ISMS equipment deployed to support nuclear non-proliferation compliance monitoring at the FMSF, Mayak. Various security assurance processes are required to provide confidence that the identified requirements adequately address and support the mission objectives of the ISMS, that the corresponding measures implemented in the equipment will meet the requirements, that the measures are implemented correctly and without flaw, that the equipment actually deployed contain the measures without alteration, that suitable on-going maintenance and other processes are in place to ensure the continued operation of the measures, and that classified information is not compromised at any time.

3.2 Differentiating Security Functions from Assurances

Any equipment will contain features in order to complete its specified purpose. Part of those features will include protection mechanisms allowing the equipment to complete its purpose without compromise of the resources contained within. The latter of these are termed 'security functions' of the equipment. In addition, the equipment has some inherent qualities that give the DTRA confidence that the features will perform as expected. These are measured through processes that assess those qualities. These are termed 'security assurances.'

It is sometimes difficult to differentiate between security features and assurances. Generally, features are equipment behavior that can be detected, tested and evaluated by interacting with that equipment, usually via the defined interface. Assurances generally are the qualitative properties of equipment, known through investigation of functional or design evidence that provides a degree of confidence the equipment can perform its functions. The mere existence of security functionality provides a certain level of confidence in the ability of the equipment to complete its mission. This document defines a *function* as a feature that is exhibited by monitoring equipment, i.e., it is something that the equipment 'does'. An *assurance* is a method by which an assessor gains confidence that the equipment truly has those features.

3.3 Assurance Combines Technical and Procedural Means

DTRA needs to have confidence that the deployed ISMS protects the monitoring information from unauthorized disclosure, modification, or deletion and that the information is available whenever it is requested. Similarly, the RF requires that the deployed ISMS protects the classified information from unauthorized disclosure. However, it is impossible to be absolutely sure that events that compromise security will not happen. There will always remain a degree of risk that security incidents will occur, either because of unforeseen circumstances, an unexpected degree of attack, or exploitation of an acceptable risk based on cost, environment factors, or perceived threat. However, the DTRA will expect that nuclear materials be monitored to the extent possible through the combination of technical and procedural means, within cost considerations. Each means will contribute to the overall goal of achieving a targeted level of confidence that the weapons origin material and monitoring information is not compromised. In the end the DTRA may need to accept some residual risk and must be prepared to take corrective action in case a security incident occurs. In order to effectively determine the amount of risk acceptable, the DTRA should conduct complete threat and risk analyses on the ISMS in order to make an informed decision on the types of equipment (and assurance in that equipment) to deploy.

Security incidents may occur either because of changing attacker incentives, an evolution in the technology available to the attacker, undetected (or known but accepted) flaws in the equipment becoming known to the attacker, or due to other unforeseen circumstances. For these reasons, the authentication of monitoring equipment should be an ongoing process. It also means that it is just as important to *know* when a compromise has occurred as to prevent one from happening.

Monitoring equipment cannot perform these functions without supporting procedures (e.g. physical access controls, periodic manual examination of equipment by inspectors). In order to gain the requisite level of confidence, the DTRA must ensure that these procedures are effective in supporting the security features of the ISMS.

Through a combination of these procedural and technological means DTRA will protect nuclear non-proliferation monitoring information in the ISMS to the extent feasible.

3.4 Framework

Standardized approaches defined in the [CC] provide input to the various life cycle phases. The requirements for security functions and assurances are developed early in the life cycle according to guidance that can be found in Part 1 of the standard, [CC1]. Part 2 [CC2], defines a menu of standard security functions that may be needed to meet security objectives (as discussed previously in subsection 2.1.2, these functions may require supporting manual components and thus may impact the operational phase as well). Part 3, [CC3], addresses assurances, that is, the verification and validation processes required to ensure that the security solutions are properly implemented, meet user requirements, and are maintained throughout the life cycle.

Functional requirements from [CC2] generally impact the design of the equipment and software. Assurance requirements from [CC3] impact the processes used to develop, test and evaluate, deploy and operate the equipment and software. People perform these processes, and thus it is important to identify the responsibility assignment for each requirement. For example, some requirements of [CC3] must be met by the developer, others by the assessor, and still others by the DTRA itself.

A balanced set of assurance measures is the best way for the DTRA to obtain the most cost-effective confidence in the ISMS. This includes expectations of the developer of this equipment, the authentication assessments made on this equipment, and the maintenance of this confidence ('continuity of knowledge') once the initial authentication assessment is complete and ISMS is used operationally. Equipment developers, independent assessors, and operational users all play a role in maintaining the confidence that weapons origin material is adequately protected and properly stored.

3.5 Authentication Assessment Reporting

The Common Evaluation Methodology document [CEM] has been issued as a companion to the Common Criteria as an agreed methodology for performing information security assessments according to the [CC]. As part of this methodology, it provides a general framework for technical reporting on these assessments. The [CEM] identifies the use of specific reports to permit the consistent reporting of evaluation results. The Observation Report (OR) is used to request clarifications (e.g. from the DTRA or the developer) or to identify a problem with an aspect of the evaluation. Observation Reports are always produced for products failing their assessment. The Evaluation Technical Report (ETR) is used to document the technical justification for the assessment verdict. The [CEM] defines minimum content for these reports, and this definition can be augmented by the DTRA to add any missing DTRA-specific required content. In general, the [CEM] requires that an assessor enumerate the activities undertaken to gain the requisite confidence in the equipment being assessed. These are directly derived from the

assurance requirements as defined by [CC3]. The assessor then provides a pass/fail verdict on whether the equipment meets each requirement and provides a justification as to why that verdict was reached. PNNL proposes to model their authentication reporting on this process.

There may be instances in which reporting how a flaw was discovered would disclose information about an evaluator's capabilities that are considered sensitive. In these cases, the flaw may be reported without discussing the methods used to detect it.

3.6 Key Roles and Responsibilities

3.6.1 DTRA Oversight

DTRA has the role to define and oversee the technical content and quality of security assessments of the security of IT monitoring equipment and software. They define the policies and technical criteria by which the ISMS will be judged, and assure that the assessments are performed in a technically sound manner, to the extent necessary to meet US needs.

DTRA has the authority to judge whether or not an identified flaw is serious enough to make the equipment unsuitable for monitoring use or if it can be successfully overcome by operational or other measures.

DTRA also retains the units that were used in the authentication assessment to be used as standards to facilitate the identification of any changes in hardware delivered for operational use.

3.6.2 Equipment Developers

The following are general developer requirements for ISMS:

1. The developer must receive sufficiently clear requirements for ISMS functionality,
2. The developer should follow proper development methods,
3. The developer should provide the level of documentation needed to effectively and efficiently assess the vulnerabilities of ISMS,
4. The developer should ensure that sufficient information is provided with the equipment so that ISMS can be used correctly,
5. The developer should make a commitment to maintain and support the assurance of the equipment over a reasonable life cycle for the equipment. This commitment should be supported through the provisioning of spares and simultaneous random selection by DTRA inspectors from spares of replacement parts and re-authentication targets. Any other modification to ISMS will require complete re-authentication, and
6. The developer must notify the DTRA of any changes made to the ISMS during its life cycle. If the changes involve any security critical components that have been identified by the developer or the authentication assessors (the entire system), they must notify the DTRA and support any assessment that the DTRA deems necessary.

3.6.2 Authentication Assessors

The DTRA will receive an authentication assessment on ISMS from authentication experts who follow a general set of assessment criteria prepared for DTRA. These assessments will be based on the [CC] and [CEM] in order to ensure measurable results and a reusable process. The assessors will take into account the presumed threats, DTRA policies, and agreed assumptions about the threat environment. This combination determines the strength that the ISMS must demonstrate.

The assessment team is comprised of experts knowledgeable in the technology, the assessment criteria, and the general needs of the DTRA. To ensure an unbiased result, these assessors are independent from the specification of and development of the ISMS. While this generally requires that the assessment team be uninvolved in the design and development of the technology being assessed, in the case of the ISMS the authentication team has requested to be involved in review of design and development progress to detect early any problems with development methodology and quality of deliverables (e.g., design documentation, source code complexity, configuration management practices). The authentication assessors should be from a different organization than any involved in the development.

3.6.3 Operational Users

The ISMS operational environment must be understood, in realistic terms, including the degree of hostility in the environment. The equipment is operated in an environment not entirely under the control of DTRA. There are varying degrees of insider threats to be considered.

However, all operational users need clear instructions on the use of the equipment, and in maintaining a security environment for the equipment. Ensuring that these instructions are followed is a DTRA oversight responsibility.

The operational users are a major source of the environment and threat for the ISMS.

3.6.4 Inspectors

DTRA inspectors will periodically visit the Mayak facility for approximately two-weeks per visit. Only during their visits is the ISMS operated. Current plans call for the ISMS and the room in which it is located to be tagged and sealed by these inspectors at the conclusion of each visit. This plan may change to allow shared access to the ISMS room. Various re-authentication procedures are being developed to ensure that the ISMS remains uncompromised.

4 ASSURANCE MEASURES

4.1 Standardized Approach

The ISO/IEC 15408, Common Criteria, [CC] was developed as a collaborative effort among those nations producing information technology (IT) security certificates. The [CC] was accepted as an international standard in 1999 and is used worldwide as the means for specifying and measuring the security attributes of IT equipment and software.

In addition, the [CC] is further supported by a recognition arrangement among fourteen nations. This arrangement provides a means to assure that each of the certificate-producing schemes produces technically correct and complete evaluations, and that they report those findings in a consistent manner. Such international acceptance provides DTRA with confidence that the CC methodology is up-to-date and widely accepted.

The Common Criteria is adopted by the US and an effort is underway in the Russian Federation to adopt it. Although Belarus has also been active in the CC community, there are no members of the FSU other than Russia known to be actively pursuing adoption of the CC at this time.

4.2 Assurance Package Concept

This document uses the [CC] central concept of 'assurance packages' to define the degree of confidence required of monitoring equipment and the assurance measures that provide the required level of confidence. The [CC] provides seven example evaluation assurance levels (EALs), as well as a set of composition rules for refining those packages to meet the needs of the user. These rules include a means to provide assurance measures beyond those defined in the [CC] so that users such as DTRA may provide the specific additional measures necessary for the protection of monitoring materials and information. Therefore, the EALs are used as the starting point for authentication assessments that are defined here for application to DTRA needs, but additional measures are used to supplement their application. In addition, the [CC] terminology has been refined, where appropriate, to relate it to the DTRA environment.

4.3 Role of Assurance Measures

The [CC] provides a set of assurance requirements for use in defining the authentication assessment needs of DTRA. The following section explores the classes of assurance requirements as defined in the [CC] and relates them to the general DTRA requirements.

The requirements below are separated into what is required of the developer-produced materials, what is required of the assessor-produced materials, and what ongoing requirements must be in place during (observed) operations and which can be verified via inspections.

4.4 Control over the configuration of the equipment

It is important that ISMS be identifiable as the version that matches the design that was meant to meet the functional requirements. The existence of a strong configuration management system ensures that unknown, unauthorized additions and changes were not made in the development of the equipment.

Because of this, the ISMS should meet the following configuration management requirements:

Developer Requirements

4.4.1 The equipment should be easily, and uniquely identifiable
4.4.2 All relevant equipment-related documentation should be covered by a configuration management plan and be part of a configuration management system.
4.4.3 A list of configuration items should be maintained.
4.4.4 It should be clear that a developer is following the plan and that the plan is adequate to ensure that the equipment is in fact the right one(s).

In addition, the effort to produce and maintain evidence about the security of the equipment should also be maintained under configuration management.

4.4.5 Each piece of evidence should be clearly identifiable and clearly denote the version of the equipment being assessed.
4.4.6 It should be clear that only authorized changes to the evidence were made and that the final version of the evidence represents the equipment being assessed.

In future, for more critical and more robust monitoring systems, the configuration management system should have automated support to help ensure that the rules and controls for changes to the equipment are enforced.

Assessor Requirements

It is also important that the assessor manage the production of their report(s), and any actions agreed in the course of the assessment. In the end, the assessor must ensure that their report reflects the state of the equipment in question.

4.4.7 The assessor should use a configuration management system to manage changes to the assessment report.
4.4.8 The assessor's configuration management system should assure that any agreed activities and decisions made in the course of the evaluation and the production of any reports on the security state of the equipment in question are correctly reflected in the report.

Ongoing Operational Requirements

In addition, inspections need to verify that correct versions of the equipment continue to be used. This may be performed through functions within the equipment or through a series of procedures that an inspector may take to ascertain the version being used.

4.4.9 The inspector should be provided a means to determine the configuration of the equipment during operation.

4.5 Confidence the Equipment was the One Shipped and it is Installed Correctly

It is important that DTRA be sure that any equipment delivered has not been tampered with and can easily be brought into the secure configuration agreed for the environment at hand.

Developer Requirements

4.5.1 DTRA should have a means to ensure that equipment received is truly from the developer and that it has not been tampered with en route.

4.5.2 ISMS should be pre-installed with the appropriate secure configuration or should include adequate information for the site to properly install this configuration, and to know that the equipment is in a suitable state for use according to agreed policies.

4.5.3 The developer should provide information as to what assessment evidence (documentation, source code, complete ISMS, etc) will be delivered and when it will be delivered. Each piece of evidence must be clearly identified.

4.6 Confidence Through the Process of Development

A contention in assessment has always been the availability of internal development design information and source code. This information is necessary for assessors to completely analyze the equipment and any flaws within the equipment. The analysis of this information is often very costly, as the assessors need to spend time understanding the internals of the equipment. To lessen this cost, the ISMS authenticators have recommended that the design and code not be complex, that the operating system in ISMS have a very small footprint, and that the authentication team participate in design reviews for early detection of problems with the quality and thoroughness of design and code.

4.6.1 Availability of Design Documentation for Inspection Purposes

The more design documentation made available to the assessors, the more understanding they may gain in the inner-workings of the equipment, allowing them to have a more thorough testing and vulnerability assessment approach. Often the design is broken into three levels of abstraction, each providing more information.

1) The functional specification provides details on how a user accesses the equipment through interfaces, either direct user interfaces (commands, buttons, etc.) or programming interfaces (system interfaces). This specification will be available from the developer as part of the agreed contract for development of ISMS.

2) The high-level design provides more information on how the equipment is structured and how the different portions work together. This is often called the system architecture.

3) The detailed design organizes the internal workings of the equipment into modules with interrelationships. This detailed statement of the equipment design provides a complete look at the behavior of the internal and external interfaces and dependencies among modules. It provides a complete picture as to the inner workings of the equipment.

Design information allows the assessors the ability to gain enough understanding of the design of the equipment to thoroughly test it and assess potential security flaws.

Developer Requirements

4.6.1.1 The ISMS developer should follow good and sound development practices.

The assessor will determine that the development practices are suitable by reviewing the design of the equipment to ensure that it reflects the purpose of the equipment.

4.6.1.2 The developer should provide the authentication team with a description of the external interfaces to the ISMS, including the purpose and method of use of each. This description should be to the level of detail such that the user may use the defined interfaces to integrate the equipment into an overall system.

4.6.1.3 The developer should provide the authentication team with a description of the structure of the ISMS, including how the information barrier functions are provided.

4.6.1.4 The developer should provide the authentication team with a description of internal workings of the equipment, including the interrelationships among the modules comprising the equipment.

4.6.2 Confidence Gained by Inspecting the Source Code

The source code generates the executable code for the equipment. The term 'source code' here is used loosely as it may contain hardware, software and/or firmware. The source is central to assessing the vulnerabilities of a piece of equipment and to see the actual implementation of the design.

The resources required to analyze the source code can be substantial. Because of this, the authentication team may look at a subset of the code and extrapolate that the rest has the same quality as the sample. They will minimally look at especially critical portions of the source code as defined by analysis of detailed design and comparison to the source code tree.

For the ISMS the following apply.

Developer Requirements

4.6.2.1 The authentication team should determine which portions of the equipment are critical enough to warrant the extra work of looking at the lowest level abstraction of the design.
4.6.2.2 The developer should provide the 'source code' of the entire system.
4.6.2.3 The assessor should determine that the source code reflects the design expected.

4.6.3 Confidence Gained Through Limiting Code Complexity

One way to minimize errors in the implementation is to design it such that each module is small and is minimal in complexity. An assessor can then more easily gain an understanding of the system implementation and can more easily find flaws in that implementation. These requirements cause a developer to design and implement in a specific manner and must be done from the onset of the development. Few developers meet these types of requirements with reused code, either from internal or external sources. Therefore, these requirements are expensive to implement and developers rarely will take these requirements on board without substantial subsidy. However, DTRA should require that the ISMS developer change their development process so as to limit code complexity.

4.6.3.1 The ISMS developer should use structured development techniques to ensure that the details on the design can be well understood.

4.6.3.2 Confidence That All Levels of Abstraction Meet Requirements

It is not uncommon that, as a design is refined, decisions cause variances so that in the end the final implementation does not meet the initial intent. To avoid this, a developer should always check to see that a lower level of abstraction meets the higher one and should also perform a sanity check that (at least the lowest) level of abstraction still meets the initial requirements. The important result of this activity is to ensure that deviations in the design have not resulted in equipment that does not meet its original requirement set.

4.6.3.3 The assessor should determine that the final implementation corresponds to the original set of requirements for that equipment.

4.6.3.4 Provision of an Overall Equipment Security Policy Model

In addition, a long list of functional requirements (or functions) often does not convey the whole picture of what protection given equipment is attempting to accomplish. To aid in this it is useful to gather all the security information into a written statement of the security policy for the equipment as a whole. This is called the security policy model. There may be times when an informal description of the equipment security policies will be helpful in understanding the security objectives of the equipment. However, usually this will be self-evident with many of the equipment so is not always necessary.

4.6.3.5 The developer should provide a succinct statement of the security policies supported by the equipment, in a natural language format.

4.6.4 Documentation Delivered with the Equipment

It is imperative that users of the equipment know how to use the equipment securely. In addition, those assigned administrative duties over keeping the equipment operational also must know how to perform those duties. Both operational and administrative users must be provided with clear usage manuals that both explain what they must do and sufficient information to understand the security in their environment. These should be consistent with, and directly linked to, the agreed ISMS policies.

Developer Requirements

4.6.4.1 The developer should provide (to both DTRA (including the authentication team) and to the operational users) all information necessary to operate the equipment in a secure manner.

4.6.4.2 The developer should provide (to both DTRA (including the authentication team) and to the operational sites) all information necessary to configure and maintain the equipment in a secure manner.

4.6.4.3 All operational documentation should be written in a way that it is easy to understand and implement.

In addition, the operational sites must be provided documents on maintaining the environment of the equipment, including physical and personnel aspects of maintaining the ISMS. DTRA will largely define this information, although portions may be provided by the developer or developed through separate contractual and policy arrangements.

DTRA Requirements

4.6.4.4 DTRA should supplement developer operational documentation with DTRA-specific information on the secure operation of the equipment.

Inspector Requirements

4.6.4.5 The inspectors should ensure that the ISMS is configured in a secure manner during ongoing operations.

4.6.5 Assurance Gained Throughout the Product Life Cycle

Although configuration management is an important component of determining that the equipment is the version it is thought to be, there are other measures that can be taken to better ensure the integrity of the equipment over its lifecycle. The developer should use well-defined tools (such as compilers) that do not

introduce security problems in their use. The verification of these tools is not always possible, but if they are at least understood, the risk of them introducing vulnerabilities is minimized. It is reasonable for DTRA to require that the ISMS developer have the means to protect the materials during the development and production of the equipment. However, it is not reasonable for DTRA to require that the developer prove that the tools used in the development be without fault.

In order to ensure that no surreptitious entries are made into the equipment implementation, the developer should have security measures to control access to the implementation.

Developer Requirements

4.6.5.1 The developer should employ methods for protecting the integrity of the ISMS during development and production.
4.6.5.2 The developer should ensure that these methods are followed at all times.
4.6.5.3 The developer should use well-defined tools and techniques in the development of the equipment.

4.6.6 Testing

Both the developers and the authenticators need to test the equipment to ensure that it works as expected. There are two types of testing: positive testing to ensure that the equipment provides the functions that it claims to provide and negative testing to ensure that, while using those functions, the security of the equipment is not compromised in some way.

Developer Requirements

The developer should have a clear plan for ensuring component, integration and system testing of the equipment. These tests should be documented and repeatable so that the same test produces the same results (with some variance based on system variables). The testing should demonstrate that the equipment design (as documented) is reflected in the actual implementation this provides confidence that design decisions have not introduced any faults or vulnerabilities in the equipment. These tests are called functional tests.

4.6.6.1 The developer should have a clear test plan to ensure that all portions of the ISMS are tested.
4.6.6.2 The developer should thoroughly test all the interfaces to ensure that they behave correctly.

Authenticator Requirements

Authenticators should also perform testing of the ISMS, taking into consideration the tests that the developer performed. They will use the knowledge gained from looking at the development documentation to create their own plan and tests, performing both positive and negative testing. They should also have a clear plan for testing the equipment, both for functionality and for vulnerabilities in the equipment.

The assessors should use the developer tests as a starting point to their testing, supplementing them as necessary. For critical monitoring equipment, this testing should be comprehensive, covering all the interfaces and execution paths. However, the assessor should consider the diminishing returns in this comprehensive testing. At one point more testing will only provide negligible additional confidence in the security functions of the equipment.

4.6.6.3 The assessor should have a clear test plan to ensure that all portions of the equipment are tested.
4.6.6.4 The assessor should test the equipment interfaces to ensure that they behave correctly.
4.6.6.5 The assessor should test the equipment to determine if there are ways to circumvent the security of the equipment.

Ongoing Operational Requirements

DTRA should provide a test suite to the inspectors in order for them to determine that the ISMS is in a secure state while in operation.

4.6.7 Authentication of the ISMS

The authenticators will use all the knowledge gained through the other assurance measures to determine what, if any, flaws ISMS will have in its operating environment. They will determine whether the functions provided are strong enough to meet the threats and whether there are ways that the equipment can be misused to compromise the information stored and transmitted.

The authenticators should enlist the developers in this search for flaws. The developer should show that they have considered the applicable vulnerabilities that their equipment could contain and how they have ensured that the weaknesses have been minimized. If the developer has not done this, the authenticator will need to spend much more time analyzing these possibilities. However, the analysis of any flaw in the ISMS will remain primarily the task of the authentication team.

Developer Requirements

4.6.7.1 The developer should take vulnerability information into account in the design and implementation of the ISMS, making design choices to minimize the number of vulnerabilities.

4.6.7.2 The developer should be able to demonstrate the method by which they countered the possible vulnerabilities in the ISMS. (This may be unrealistic but it is desirable.)

Assessor Requirements

4.6.7.3 The authenticator should analyze all information provided on the equipment to determine if potential flaws exist in the operational environment.

4.6.7.4 The authenticator should produce a thorough and systematic plan for determining residual flaws in the equipment.

4.6.7.5 The assessor should investigate (through testing or analysis) to see if such flaws exist.

4.6.7.6 The assessor should fully document all the results of the analysis and testing as to which flaws exist, and the conditions under which they exist. This should also include enough information for DTRA to determine the severity of the flaws and whether other measures can be taken to satisfactorily mitigate them.

4.7 Establishing Authentication Assurance Levels

The general assurance requirements outlined above has been translated into a set of assurance packages, as outlined in the [CC]. The [CC] has seven predefined assurance packages, known as Evaluation Assurance Levels (EALs). These provide balanced groupings of assurance components that are intended to be generally applicable. The seven EALs are as follows:

- EAL1 - functionally tested
- EAL2 - structurally tested
- EAL3 - methodically tested and checked
- EAL4 - methodically designed, tested and reviewed
- EAL5 - semiformally designed and tested
- EAL6 - semiformally verified design and tested

- EAL7 - formally verified design and tested

These EALs are used as a set of baselines in the assessment of general information technology by national evaluation and certification schemes for inclusion on Evaluated Products Lists (EPLs) as an aid in purchasing these technologies for inclusion in operational systems. Most commercial evaluations target somewhere between EAL3 and EAL4 as an assurance package. However, these are used only as baselines and many assessments of commercial products include additional assurance measures to these levels: these are usually termed 'EAL augmented.'

Although a good basis for DTRA authentication campaigns, the EALs only provide assurance through the development of equipment; assurance gained and maintained during the operations of the equipment, by those performing the operations, is not discussed by the [CC].

PNNL has developed five assurance packages for use in authenticating monitoring equipment. These are termed Authentication Assurance Levels (AALs). The application of these AALs is largely a DTRA management decision, but should be based on a reasonable and appropriate combination of threat to the equipment in the monitoring environment and budgetary considerations. PNNL proposes AAL3 as an appropriate target for the ISMS. Given that CC acceptance and knowledge in the RF is limited at this time, it is difficult to communicate in a timely and effective manner to the developer the higher requirements of AAL4.

4.7.1 AAL0 - Unauthenticated

AAL0 is applicable where no confidence in the correct operation can be expected due to the lack of assurance measures taken by the developer or authenticating authority. This AAL is used where, although some assurance measures might have been used, none are sufficient to provide any measure of confidence in system operations. For example, the developer does not develop, provide, or maintain any of the documentation on system design, development, and operations, nor does the developer allow members of the authenticating authority to participate in system design review, or to witness a comprehensive test of the system.

4.7.2 AAL1 - Minimally Authenticated

AAL1 is the minimum level of assurance that any equipment used in monitoring regimes should have. An authentication at this level should provide evidence that the Target of Authentication (TOA) functions in a manner consistent with its documentation, and that it provides useful protection against identified threats. Co-operation of the developer is required in terms of the delivery of design information and test results.

AAL1 is applicable in those circumstances where developers or users require a low level of independently assured security in the absence of ready availability of the complete development record. The developer conducts functional and high-level design testing, and independent testing is conducted to ensure only that security functions perform as specified.

4.7.3 AAL2 - Limited Authentication

AAL2 is applicable in those circumstances where developers or users require a moderate level of independently assured security and are prepared to incur additional security-specific engineering costs. AAL2 requires the co-operation of the developer in terms of the delivery of design information and test results.

AAL2 requires additional components from each of the Security Assurance Requirement classes except guidance documents. Authentication analysis is supported by the low-level design of the modules of the TOA, covert channel analysis and a subset of implementation of the TOA Security Functions. Development controls are supported by a life-cycle model, identification of tools, and partially automated configuration management.

4.7.4 AAL3 - Critical Authentication

This AAL is applicable where there is a need for higher level of independently assured security in a planned development, and a requirement for a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques. AAL3 is the recommended lowest assurance level that any equipment used in monitoring regimes should have.

AAL3 requires that the system be highly resistant to exploitation. A developer designed lifecycle model, the tracking of security flaws, and independent testing of a selected sample of developer tests enhances assurance.

4.7.5 AAL4 - Optimal Authentication

AAL4 is the maximum level of assurance economically possible for equipment used in monitoring regimes. It is applicable where the value of the protected assets justifies the additional costs. AAL4 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOA for protecting high value assets against significant risks.

AAL4 provides complete automation of configuration management, prevention of modification and compliance with implementation standards. Semi-formal responses from the developer are required for functional specifications, high-level design documentation and the TOA security policy model. The independent vulnerability assessments must ensure the system's resistance to attackers. The developer must conduct a systematic search for covert channels, and test the low-level design. Development environment and configuration management controls are further strengthened.

5 STRATEGIES TO MINIMIZE AUTHENTICATION COSTS

5.1 Early Integration of Security Requirements

The integration of security functional and assurance requirements early in the product life cycle will lead to overall lower life cycle costs.

The early identification of functional security requirements will permit system designers to more fully understand user needs and will allow trade-off studies to be developed which address overall life cycle costs, including assessment costs, and which consider the full range of hardware, software and manual options.

The early integration of assurance requirements into project planning will ensure that the measures and deliverables needed are fully identified up-front to all parties, and will ensure that unexpected requirements, costs or project delays do not arise later in the project. Early involvement of the assessors in the design process (e.g. by performing concurrent assessment) can provide the developer with early feedback on the attainment of the functional requirements and compliance with the assurance

requirements. (However, care should be taken in order that the assessors maintain sufficient independence from the actual development.)

The identification and publication of the Protection Profile (PP) will provide essential input to the developer. These documents will identify the security functions which must be included in the product to be developed and will define to the developer the level of rigor which must be applied to the development process and corresponding documentation. PNNL is separately developing a protection profile based on the ISMS functional requirements.

With the early identification of functional requirements, system designers can more fully understand user needs and examine options that span the full range of hardware, software and manual procedures. Options can be analysed which identify overall life cycle costs, including development and assessment costs, and develop trade-off studies between the options available. PNNL recommends release to the ISMS developer of DTRA's functional and assurance security requirements, so that the developer can better understand and comply with these requirements.

5.2 Early Input to Functional Design

Because the ISMS is being developed for DTRA under contract, it is recommended the authentication team participate in proposal review and design reviews. The objective is to improve the authenticatability of the final product by identifying quality issues in the various levels of abstraction (e.g., proposed functional design, high-level design, detailed design) of the ISMS as early as possible in the development process. Early detected problems can be affordably corrected.

5.3 Role of COTS Components

Where a particular solution can be constructed using commercial off the shelf (COTS) components, it may be feasible to reduce overall authentication costs to the extent COTS products may be reasonably trusted. For example, it may not be necessary to examine the source code for a COTS operating system from a non-Russian developer. For such components, it should be sufficient to verify by a bit compare process that the operational component is identical to the commercially available product (purchased under a blind buy).

6 CONCLUSIONS AND RECOMMENDATIONS

The following issues are recommended for further study.

6.1 Define Security Policies and Procedures

DTRA should provide a written set of security policies and procedures so the authenticators can assure that the equipment can meet those policies, and operate under the procedures. Existing policies and procedures should be reviewed and revised as necessary. This review is an ongoing task as the threat environments are likely to evolve over time. In addition, these policies and procedures should include how and when they are applied, and the circumstances under which they may be waived.

6.2 Define Security Functional Requirements

Assurance measures alone are not sufficient for ensuring the protection of monitoring information. In fact, they are meaningless without a set of security functional requirements against which to assess equipment. DTRA should produce a set of complete IT security requirements in the form of "Protection Profiles" and release them to authenticators to ensure that the authenticator can verify that the functional requirements have been correctly implemented, and to developers, to ensure that they have a clear statement of the security functional requirements for an equipment that can meet DTRA needs.

6.3 Define Acceptable Approach(es) to Meet Assurance Requirements

There are numerous ways in which a developer might well meet some of the assurance requirements such as configuration management or development method. DTRA should define, by way of "examples", the approach(es) that are acceptable, which may be based on experience with previous equipment.

6.4 Authentication Reports

DTRA should develop a clear guidance document on the format, structure and content of assessment (as well as inspection) reports. [CEM] is an excellent source for this purpose.

7 REFERENCES

[CC]	Used to refer to all of: [CC1], [CC2], and [CC3] (see below).
[CC1]	ISO/IEC 15408-1:1999, Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1 Introduction and General Model.
[CC2]	ISO/IEC 15408-2:1999, Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 2 Security Functional Requirements.
[CC3]	ISO/IEC 15408-3:1999, Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3 Security Assurance Requirements.
[CCRA]	ARRANGEMENT on the Recognition of Common Criteria Certificates In the field of Information Technology Security, May, 2000 (*can we cite this – it is an un-numbered document*)
[CEM]	Used to refer to all of: [CEM1] and [CEM2] (see below).
[CEM1]	Common Evaluation Methodology for Information Technology Security, Part 1 - Introduction and general model, Common Criteria Project, January 1997.
[CEM2]	Common Evaluation Methodology for Information Technology Security, Part 2 - Evaluation Methodology, Common Criteria Project, August 1999.
[CMMI]	Used to reference both documents cited below: 1) Capability Maturity Model – Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development (CMMI-SE/SW/IPPD), Staged Representation, Version 1.02, Software Engineering Institute, Carnegie Mellon University, November 2000. 2) Capability Maturity Model – Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development (CMMI-SE/SW/IPPD), Continuous Representation, Version 1.02, Software Engineering Institute, Carnegie Mellon University, November 2000.
[EN45000]	Series of Euronorm standards for the mutual recognition of laboratories EN 45001: General criteria for the operation of testing (see [ISO17025]) EN 45002: General criteria for assessment of testing laboratories EN 45003: General criteria for laboratory accreditation bodies
[IEEE12207.0]	IEEE/EIA 12207.0-1998, Industry Implementation of International Standard ISO/IEC 12207:1995, Software Life Cycle Processes, March 1998 (includes complete text of [ISO12207])
[IEEE12207.1]	IEEE/EIA 12207.1-1997, IEEE/EIA Guide for Information Technology, Software Life Cycle Processes - Life Cycle Data, April 1998.
[IEEE12207.2]	IEEE/EIA 12207.2-1997, IEEE/EIA Guide, Software Life Cycle Processes - Implementation Considerations, April 1998.
[ISO12207]	ISO/IEC 12207:1995, Information Technology, Standard for Software Life Cycle Processes (see [IEEE12207.0]).
[ISO15288]	ISO/IEC JTC1/SC7 N2257 2nd Committee Draft, Information Technology - Life Cycle Management - System Life Cycle Processes, January 21, 2000.
[ISO17025]	ISO/IEC 17025:1999, General requirements for the competence of testing and calibration laboratories (previously known as ISO Guide 25).
[Kouzes2001a]	Authentication Of Radiation Measurement Systems For Non-Proliferation, Richard T. Kouzes, Bruce Geelhood, Randy Hansen, W. Karl Pitts, PNNL Report PNNL-SA-3487, May 2001

[Kouzes2001b] Authentication Assurance Levels: Strategy For Applying The Iso Common Criteria Standards, R. T. Kouzes, J.R. Cash, R.R. Hansen, D.M. Devaney, Report PNNL-SA-xxxxxx, July 2001

[Kouzes2001c] Authentication Procedures, Richard T. Kouzes, Leigh Bratcher, Tom Gosnell, Diana Langner, Duncan MacArthur, John Mihalczo, Carolyn Pura, Alex Riedy, Paul Rexroth, Jay Spingarn, Mary Scott, Report PNNL-13550, May 2001

A ANNEX: COMMON CRITERIA ASSURANCE PACKAGES

A.1 Introduction

Table A-1 provides a general view of the five proposed AALs for DTRA equipment. A description of the specific activities follows for AAL3 (recommended for ISMS), using the standard language of the CC. Application notes to aid in the specific application of the assurance measures for DTRA purposes are also provided.

The requirement statements in the specific activities sections below use the CC terminology. This means that the requirements are divided into three sections: requirements for evidence on the equipment, the contents of that evidence (or the information that the authenticator needs to glean from the evidence), and the action that the authenticator will take to confirm that the evidence is adequate. For the last of these, there is a generic statement that the 'Evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.' This simply means that the authenticator confirms that the developer has met all their requirements.

Because the requirement statements use the CC terminology, a simple mapping of this terminology to DTRA terminology can be made. Therefore, for all these requirements the following use of terminology can be assumed:

- The term 'TOE' can be read as 'monitoring equipment'.
- The term 'TSF' can be read as the 'security functions in the monitoring equipment'.
- The term 'evaluator' can be read as 'DTRA authenticator'.
- The term 'developer' can be read as 'equipment developer or agent employed to develop evidence'.

A.2 Conventions in the DTRA Authentication Assurance Levels

Table 1 provides a summary overview of the types of assurance measures applicable at each of the EALs defined in the [CC] and for AAL3 for DTRA use (the remaining AALs will be completed in detail in the future). It provides an overview for the purposes of comparison. The reader should reference the [CC] for further explanation of the labeling conventions used. The contents of the requirements are expanded in the sections that follow Table 1. With those expanded requirements are references to the source of the [CC] requirements for comparison purposes. Note that these are references to the first occurrence of the requirements with a [CC] family and requirements are not repeated within a given table of requirements. For those instances where the [CC] is extended or expanded, a naming convention of 'EXP' is appended to the element reference. (The [CC] calls these 'explicitly stated requirements').

An asterisk (*) is included with the number when further explanation is provided for use within DTRA developments. These further expansions of the assurance measures are provided in the 'Application Notes' sections that follow. These may not always be applicable when DTRA is choosing a COTS piece of monitoring equipment. However, they can be applied in developments and authentication regimes under the control of DTRA.

It is important to note that all information on the application of the [CC] cannot be replicated here. The DTRA, assessors and developers should refer to the [CC] and the [CEM] to gain more information. In addition, they should monitor the process of interpreting the standard on the [CC] project website http://www/commoncriteria.org.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level											
		EAL (from CC)							Authentication Assurance Level (AAL)				
		1	2	3	4	5	6	7	**0**	**1**	**2**	**3**	**4**
Configuration management	ACM_AUT				1	1	2	2				**1**	
	ACM_CAP	1	2	3	4	4	5	5				**4**	
	ACM_SCP			1	2	3	3	3				**2**	
Delivery and operation	ADO_DEL		1	1	2	2	2	3				**2**	
	ADO_IGS	1	1	1	1	1	1	1				**1**	
Development	ADV_FSP	1	1	1	2	3	3	4				**2***	
	ADV_HLD		1	2	2	3	4	5				**2***	
	ADV_IMP				1	2	3	3				**1***	
	ADV_INT					1	2	3					
	ADV_LLD				1	1	2	2				**1***	
	ADV_RCR	1	1	1	1	2	2	3				**1**	
	ADV_SPM				1	3	3	3				**1***	
Guidance documents	AGD_ADM	1	1	1	1	1	1	1				**1**	
	AGD_USR	1	1	1	1	1	1	1				**1**	
Life cycle support	ALC_DVS			1	1	1	2	2				**1**	
	ALC_FLR												
	ALC_LCD				1	2	2	3				**1***	
	ALC_TAT				1	2	3	3				**1**	
Tests	ATE_COV		1	2	2	2	3	3				**2**	
	ATE_DPT			1	1	2	2	3				**1***	
	ATE_FUN		1	1	1	1	2	2				**1***	
	ATE_IND	1	2	2	2	2	2	3				**2***	
Vulnerability assessment	AVA_CCA					1	2	2				**1***	
	AVA_MSU			1	2	2	3	3				**1**	
	AVA_SOF		1	1	1	1	1	1				**1**	
	AVA_VLA		1	1	2	3	4	4				**4***	
Assurance Maintenance	AMA_AMP												
	AMA_CAT												
	AMA_EVD												
	AMA_SIA												
** Includes elements refined or added to meet specific DTRA needs.*													

Table 1: Summary of CC and ISMS Authentication Assurance Levels

A.3 Control over the Configuration of the Equipment Objectives

By controlling the configuration definition and changes during development, it can be assured that the resulting equipment reflects the design requirements and is tested to those requirements. This is accomplished through a combination of an agreed scope over what items should be under change control, the rigor of the configuration management control system, and the degree of automated support to that process.

A.3.1 Application Notes

A.3.1.1 Scope of the Configuration Management System

The [CC] (in ACM_SCP.1) requires the following as the required configuration items under configuration control: TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation and CM documentation. The coverage of other documentation, such as the vulnerability analysis documentation, is not explicitly covered. Although this may be acceptable, in the DTRA context, for generally applicable commercially available equipment, the list of those items covered by the configuration management system may be negotiated with the developer for specialty monitoring equipment. In particular, this list may not be applicable to all equipment or it may not be cost effective to place all items under control.

The entire list of configuration items required in the [CC] may not be applicable to all monitoring equipment and may therefore be a matter of negotiation in the initial contract with the developer. However, it is imperative that the complete list be fully defined to ensure that the developer knows what needs to be covered by the configuration management system.

In addition, the developer may choose to control changes to some configuration items via different systems. In this instance, the methods would be differentiated in the configuration management documentation and the configuration items covered by each method would be identified.

A.3.1.2 Identification of the equipment (TOE) version

The CC requires that a reference be provided for the TOE so the consumer can identify when they have the evaluated version of that TOE. It is also important that all relevant documentation also carry that same reference so that the assessor, and DTRA as the consumer; can match the documentation with the evaluated version of the equipment being used in monitoring.

A.3.1.3 Evaluator confirmation of configuration management system

The CC requires that the assessor verify that the configuration management system is being effectively used and that it is adequately documented. DTRA may choose to enforce this requirement through contractual means or require the assessor to confirm the configuration management system via alternate, less rigorous means. In addition, the information required in the documentation may be obtained through a combination of written and verbal communications so the rigor of the documentation requirements may also be lessened.

Control over equipment configuration & changes during development	**AAL3**
Developer Action Elements:	
The developer shall provide a reference for the TOE. [ACM_CAP.1.4D]	**X**
The developer shall use a CM system. [ACM_CAP.2.2D]	**X**
The developer shall provide CM documentation.[ACM_AUT.1.2D, ACM_CAP.2.3D, ACM_SCP.1.1D]	**X**
Content and presentation of evidence elements:	
The CM documentation shall show that the CM system, as a minimum, tracks the following configuration items [*assignment: list of configuration items*]. [ACM_SCP.1.1C EXP1]	**X**

Control over equipment configuration & changes during development	AAL3
The CM documentation shall describe how configuration items are tracked by the CM system. [ACM_SCP.1.2C]	**X**
The reference for the TOE shall be unique to each version of the TOE. [ACM_CAP.1.1C]	**X**
The TOE shall be labeled with its reference. [ACM_CAP.1.2C]]	**X**
All configuration items for the TOE shall be labeled with the TOE's reference. [ACM_CAP.3.2C- EXP2]	**X**
The CM documentation shall include a configuration list and a CM plan. [ACM_AUT.1.2D, ACM_CAP.3.3C]	**X**
The configuration list shall describe the configuration items that comprise the TOE. [ACM_CAP.2.4C]	**X**
The CM system shall provide an automated means by which only authorized changes are made to the TOE implementation representation. [ACM_AUT.1.1C]	**X**
The CM system shall provide an automated means by which only authorized changes are made to all configuration items [ACM_AUT.2.1C]	**X**
The CM system shall provide an automated means to support the generation of the TOE. [ACM_AUT.1.2C]	**X**
The CM plan shall describe the automated tools used in the CM system. [ACM_AUT.1.3C]	**X**
The CM plan shall describe how the automated tools are used in the CM system. [ACM_AUT.1.4C]	**X**
The CM system shall provide an automated means to ascertain the changes between the TOE and its preceding version. [ACM_AUT.2.5C]	**X**
The CM system shall provide an automated means to identify all other configuration items that are affected by the modification of a given configuration items. [ACM_AUT.2.6C]	**X**
The CM system shall uniquely identify all configuration items. [ACM_CAP.2.6C]	**X**
The CM documentation shall describe the method used to uniquely identify the configuration items. [ACM_CAP.2.5C]	**X**
The CM plan shall describe how the CM system is used. [ACM_CAP.3.7C]	**X**
The evidence shall demonstrate that the CM system is operating in accordance with the CM plan. [ACM_CAP.3.8C]	**X**
The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system. [ACM_CAP.3.9C]	**X**
The CM system shall provide measures such that only authorized changes are made to the configuration items. [ACM_CAP.3.10C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ACM_AUT.1.1E, ACM_CAP.1.1E, ACM_SCP.1.1E]	**X**

A.4 Confidence that equipment is the one shipped

A.4.1 Objectives

Requiring control over the delivery procedures provides assurance that the equipment has not been tampered with via the distribution channels. At the very least, DTRA should know the way in which the equipment will be delivered so they know they have received the official version. For more critical

equipment, the distribution channels need to be controlled to prevent efforts to exchange the official version with one masquerading as that critical piece of equipment.

In addition to ensuring that the equipment received was correct, DTRA needs to control the delivery of the equipment to the operational sites.

A.4.2 Application Notes

DTRA needs to know the distribution channels of its equipment. However, it is not the goal to have pristine documentation of these procedures. Therefore, the assessor needs to verify that procedures are followed and that DTRA knows when it has received the equipment expected. Therefore, DTRA may choose to fulfill these requirements through the assessor establishing what the procedure is, and reporting that to DTRA. It also may be accomplished via contractual means and the assessor does not need to apply much rigor to the procedures.

Delivery procedure	**AAL3**
Developer Action Elements:	
The developer shall document procedures for delivery of the TOE or parts of it to the user. [ADO_DEL.1.1D]	**X**
The developer shall use the delivery procedures. [ADO_DEL.1.2D]	**X**
Content and presentation of evidence elements:	
The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site. [ADO_DEL.1.1C]	**X**
The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site. [ADO_DEL.2.2C]	**X**
The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site. [ADO_DEL.2.3C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	**X**

A.5 Confidence through the process of equipment development

A.5.1 Objectives

The more DTRA knows about the design of equipment put to monitoring use, the more they will be able to ascertain ways in which the security features of the equipment could be compromised by an adversary. Knowledge of the design helps the assessor plan for testing and identification of residual vulnerabilities by giving them clues to potential 'weak' points in the equipment design and implementation. It also means that the assessor can spend less time using 'brute force' testing techniques and can perform much of the vulnerability assessment through analysis.

There are different levels of abstraction in the design. They serve different purposes and are usually meant for different audiences. The users of the equipment, and the assessors, need to know how to interface with the equipment. These interfaces are generally provided in a functional specification. How the equipment is designed to accomplish its functions is often described in a high level design. The

details of how the design is then accomplished can then be described in a low-level design. Finally, the equipment is put together using some type of implementation representation. In traditional computing equipment this is often termed the 'source code.' Although equipment that is mostly hardware-based often does not have such source code they have some other representation that is how the design is transfigured into the actual equipment.

Having the different levels of abstraction helps an assessor understand what the equipment is trying to accomplish, and the means by which it is put together to accomplish those tasks. The more the assessor(s) understand, the more likely they will be able to have confidence that the flaws in the equipment have been minimized.

A.5.2 Application notes

A primary goal in the development of monitoring equipment is to ensure that the final implementation reflects the functional requirements laid on that equipment. It is a secondary goal to have the eventual design fully documented so the equipment can be maintained over its life cycle. Therefore, the developer should make sure that the design documentation reflects the final product and the assessor should use these documents in their search for possible flaws. However, the assessor may use verbal communication to get explanations of design questions to supplement the documentation. Although the documentation should not be in error, there should not be a necessity to change the documentation to reflect all the assessor's questions.

A major difference between the design documentation requirements is that higher levels require that the text be provided in a 'semiformal' style. This means that the terminology should be more tightly controlled, using terms and structures that avoid ambiguity in the descriptions.

A.5.3 Functional specification

The functional specification is a high-level description of the user-visible interface and behavior of the TSF. It is usually derived from user documentation that provides the form, content and effects of the means of user interaction with the equipment. The assessor will use this information to plan their interaction with the equipment, including testing through those interfaces. They will also use these interfaces to determine that all of the equipment's functional security requirements are met.

Functional specification	**AAL3**
Developer Action Elements:	
The developer shall provide a functional specification. [ADV_FSP.1.1D]	**X**
Content and presentation of evidence elements:	
The functional specification shall describe the TSF and its external interfaces using an informal style [ADV_FSP.1.1C]	**X**
The functional specification shall describe the TSF and its external interfaces using an semiformal style, supported by informal, explanatory text where appropriate [ADV_FSP.3.1C]	**X**
The functional specification shall be internally consistent. [ADV_FSP.1.2C]	**X**
The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate. [ADV_FSP.1.3C]	**X**

Functional specification	AAL3
The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages, as appropriate. [ADV_FSP.2.3C]	**X**
The functional specification shall completely represent the TSF. [ADV_FSP.1.4C]	**X**
The functional specification shall include rationale that the TSF is completely represented. [ADV_FSP.2.5C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_FSP.1.1E]	**X**
The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements. [ADV_FSP.1.2E]	**X**

A.5.4 High-level design

The high-level design of a TOE provides a description of the TSF in terms of major structural units (i.e. subsystems) and relates these units to the functions that they provide. The high-level design requirements are intended to provide assurance that the TOE provides an architecture appropriate to implement the TOE security functional requirements.

The high-level design refines the functional specification into subsystems. For each subsystem of the TSF, the high-level design describes its purpose and function, and identifies the security functions contained in the subsystem. The interrelationships of all subsystems are also defined in the high-level design. These interrelationships will be represented as external interfaces for data flow, control flow, etc., as appropriate.

High level design	AAL3
Developer Action Elements:	
The developer shall provide the high-level design of the TSF. [ADV_HLD.1.1D]	**X**
Content and presentation of evidence elements:	
The presentation of the high-level design shall be semiformal. [ADV_HLD.3.1C]	**X**
The high-level design shall be internally consistent. [ADV_HLD.1.2C]	**X**
The high-level design shall describe the structure of the TSF in terms of subsystems. [ADV_HLD.1.3C]	**X**
The high-level design shall describe the security functionality provided by each subsystem of the TSF. [ADV_HLD.1.4C]	**X**
The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. [ADV_HLD.1.5C]	**X**
The high-level design shall identify all interfaces to the subsystems of the TSF. [ADV_HLD.1.6C]	**X**
The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. [ADV_HLD.1.7C]	**X**
The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error	**X**

High level design	AAL3
messages, as appropriate. [ADV_HLD.2.8C]	
The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems. [ADV_HLD.2.9C]	**X**
The high-level design shall justify that the identified means of achieving separation, including any protection mechanism, are sufficient to ensure clear and effective separation of TSP-enforcing from non-TSP-enforcing functions. [ADV_HLD.4.10C]	**X**
The high-level design shall justify that the TSP mechanisms are sufficient to implement the security functions identified in the high-level design. [ADV_HLD.4.11C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_HLD.1.1E]	**X**
The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements [ADV_HLD.2.2E]	**X**

A.5.5 Low-level design

The low-level design of a TOE provides a description of the internal workings of the TSF in terms of modules and their interrelationships and dependencies. The low-level design provides assurance that the TSF subsystems have been correctly and effectively refined.

For each module of the TSF, the low-level design describes its purpose, function, interfaces, dependencies, and the implementation of any TSP-enforcing functions.

Low-level design	AAL3
Developer Action Elements:	
The developer shall provide the low-level design of the TSF. [ADV_LLD.1.1D]	**X**
Content and presentation of evidence elements:	
The presentation of the low-level design shall be semiformal. [ADV_LLD.2.1C]	**X**
The low-level design shall be internally consistent. [ADV_LLD.1.2C]	**X**
The low-level design shall describe the TSF in terms of modules. [ADV_LLD.1.3C]	**X**
The low-level design shall describe the purpose of each module. [ADV_LLD.1.4C]	**X**
The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules. [ADV_LLD.1.5C]	**X**
The low-level design shall describe how each TSP-enforcing function is provided. [ADV_LLD.1.6C]	**X**
The low-level design shall identify all interfaces to the modules of the TSF. [ADV_LLD.1.7C]	**X**
The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible. [ADV_LLD.1.8C]	**X**
The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects, exceptions and error messages, as appropriate. [ADV_LLD.1.9C]	**X**
The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing complete details of all effects, exceptions and error	**X**

Low-level design	AAL3
messages, as appropriate. [ADV_LLD.2.9C]	
The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules. [ADV_LLD.1.10C]	X
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_LLD.1.1E]	X
The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements. [ADV_LLD.1.2E]	X

A.5.6 Implementation representation

The description of the implementation representation in the form of source code, firmware, hardware drawings, etc. captures the detailed internal workings of the TSF in support of analysis.

Implementation representation	AAL3
Developer Action Elements:	
The developer shall provide the implementation representation for a selected subset of the TSF. [ADV_IMP.1.1D]	X
The developer shall provide the implementation representation for the entire TSF. [ADV_IMP.2.1D]	X
Content and presentation of evidence elements:	
The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions. [ADV_IMP.1.1C]	X
The implementation representation shall be internally consistent. [ADV_IMP.1.2C]	X
The implementation representation shall describe the relationship between all portions of the implementation. [ADV_IMP.2.3C]	X
The implementation representation shall be structured into small and comprehensible sections. [ADV_IMP.3.4C]	X
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_IMP.1.1E]	X
The evaluator shall determine that the implementation representation provided is an accurate and complete instantiation of the TOE security functional requirements. [ADV_IMP.1.2E]	X
The evaluator shall determine that the least abstract TSF representation is an accurate and complete instantiation of the TOE security functional requirements. [ADV_IMP.2.3E]	X

A.5.7 Complexity of the internal design

Requirements on the minimization of the complexity of the design allows an assessor to more easily understand the equipment and all the ways it could be used both, including ways to circumvent the security features. It imposes some techniques to help ensure that the equipment is as simple as practical

for that equipment type. This set of requirements is likely only to be applicable in small, very critical equipment.

The CC requires that only access control functions be simple enough to be analyzed. Access control may not generally be a critical security function in DTRA monitoring equipment. Instead it is imperative that any security function relied upon to protect the confidentiality and integrity of the monitoring information be simple enough to analyze so that potential flaws can be identified.

The requirements call for an 'architectural description'. This description is similar to the low-level design, in that it is concerned with the modules of the TSF. In fact, it would likely be incorporated in the low-level design documentation. However, this description provides evidence of the modularity and minimization of complexity of the interaction among modules while the low-level design describes the design of the modules.

Internal design complexity	**AAL3**
Developer Action Elements:	
The developer shall design and structure the TSF in a modular fashion that avoids unnecessary interaction between the modules of the design. [ADV_INT.1.1D]	
The developer shall design and structure the TSF in a layered fashion that minimizes mutual interactions between the layers of the design. [ADV_INT.2.3D]	
The developer shall design and structure the TSF in such a way that minimizes the complexity of the portions of the entire TSF. [ADV_INT.3.4D]	
The developer shall design and structure the TSF such that the [assignment: critical security functions] are simple enough to be analyzed [ADV_INT.3.5D-EXP]	
The developer shall ensure that functions whose objectives are not relevant for the TSF are excluded from the TSF modules. [ADV_INT.3.6D]	
The developer shall provide an architectural description. [ADV_INT.1.2D]	
Content and presentation of evidence elements:	
The architectural description shall identify the modules of the TSF and shall specify which portions of the TSF enforce the [assignment: critical security functions] policies. [ADV_INT.3.1C-EXP]	
The architectural description shall describe the purpose, interface, parameters, and side-effects of each module of the TSF. [ADV_INT.1.2C]	
The architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions. [ADV_INT.1.3C]	
The architectural description shall describe the layering architecture. [ADV_INT.2.4C]	
The architectural description shall show that the mutual interactions have been minimized, and justify those that remain. [ADV_INT.2.5C]	
The architectural description shall describe how the entire TSF has been structured to minimize complexity. [ADV_INT.3.6C]	
The architectural description shall justify the inclusion of any non-TSP-enforcing modules in the TSF. [ADV_INT.3.7C]	
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_INT.1.1E]	
The evaluator shall determine that both the low-level design and the implementation representation are in compliance with the architectural description. [ADV_INT.1.2E]	
The evaluator shall confirm that the portions of the TSF that enforce the [assignment: critical security functions] policies are simple enough to be analyzed. [ADV_INT.3.3E-	

Internal design complexity	AAL3
EXP]	

A.5.8 Correspondence between the levels of design abstraction

The correspondence between the various TSF representations (i.e. TOE summary specification, functional specification, high-level design, low-level design, implementation representation) addresses the correct and complete instantiation of the requirements to the least abstract TSF representation provided. This conclusion is achieved by step-wise refinement and the cumulative results of correspondence determinations between all adjacent abstractions of representation.

Correspondence between design levels of abstraction	AAL3
Developer Action Elements:	
The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. [ADV_RCR.1.1D]	**X**
Content and presentation of evidence elements:	
For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. [ADV_RCR.1.1C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_RCR.1.1E]	**X**

A.5.9 Equipment security policy model

It is possible for a piece of equipment to have several functions but not have a cohesive security policy to which each of those functions can contribute. It is often helpful to see the rules and characteristics of each security function, and to relate them to the overall security goals of the equipment. The policy statement (or model) will help the assessor see that the equipment is working as a consistent whole toward reaching its goals. A central notion in the security policy is the definition of what it means for the equipment to be in a 'secure' state'.

It is important to note that the phrase 'that can be modeled' allows the developer to negotiate with the assessor (and DTRA) to establish which policies (or equipment functions) need a description as outlined in the requirements. This is because natural language descriptions of the rules and characteristics can be produced for all the functions of the equipment. The question is then the usefulness of this complete set of descriptions. Therefore that phrase can be interpreted as policies that are 'worth modeling'.

Equipment security policy	AAL3
Developer Action Elements:	
The developer shall provide a security policy model. [ADV_SPM.1.1D]	**X**
The developer shall demonstrate correspondence between the functional specification and the TSP model. [ADV_SPM.1.2D]	**X**
Content and presentation of evidence elements:	
The TSP model shall be informal. [ADV_SPM.1.1C]	**X**
The TSP model shall be semiformal. [ADV_SPM.2.1C]	**X**

Equipment security policy	AAL3
The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled. [ADV_SPM.1.2C]	**X**
The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all polices of the TSP that can be modeled. [ADV_SPM.1.3C]	**X**
The demonstration of correspondence between the TSP model and the functional specification shall show that all the security functions in the functional specification are consistent and complete with respect to the TSP model. [ADV_SPM.1.4C]	**X**
Where the functional specification is at least semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal. [ADV_SPM.2.5C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ADV_SPM.1.1E]	**X**

A.6 Guidance documentation delivered with the equipment

A.6.1 Objectives

Guidance documentation allows those personnel, installing, configuring, maintaining and using the equipment to do so in full knowledge of the security aspects of the equipment. This guidance should be complete, consistent and should be written so that the user can easily follow the instructions therein.

A.6.2 Application Notes

Generally a developer provides usage manuals when they deliver a set of equipment. These include instructions on how to set up, install, and operate the equipment. There are generally two audiences for this documentation: those that maintain and administer the equipment (administrator) and those who use the resources of the equipment (user). Users usually needs to know a subset of what the administrator needs to know. Administrator guidance is intended to be used by those persons responsible for installing, configuring, maintaining, and administering the TOE in a correct manner for maximum security. User guidance refers is intended to be used by non-administrative users of the TOE, including those using the TOE's externals interfaces (e.g. programmers).

All requirements for guidance documentation have been combined here, although there may be a series of documentation, each geared the different audiences. Therefore, the terms 'administrator guidance' and 'user guidance' have been combined into the one term 'guidance documentation'. This is because the definition of 'user' and 'administrator' can sometimes be blurred for monitoring equipment, as operational users may only be those that configure and maintain the equipment. In addition, the purpose of these requirements is to ensure that all personnel needing to interact with the equipment have the information they need to do so securely. The type and usage of the equipment will dictate how many documents that will need to be. Therefore, whenever the term 'authorized user types' is used it is meant to capture both classical roles of administrators and operational users. It also captures the notion that different types of users may require different information and requires that each user have the information necessary to complete their assigned tasks.

Installation, generation and start-up procedures are often considered part of the administrator guidance but are of a different type of information that may be used by different personnel. The administrator guidance addresses those things that a user needs to know in maintaining the equipment in its operational environment. Installation guidance contains information on setting the equipment up in the first place.

Usage guidance documentation	**AAL3**
Developer Action Elements:	
The developer shall provide guidance documentation addressed to each authorized user type. [AGD_ADM.1.1D, AGD_USR.1.1D, AVA_MSU.1.1D - **refined**]	**X**
The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. [ADO_IGS.1.1D]	**X**
The developer shall provide the TOE pre-installed in the [assignment: defined secure state for the DTRA environment]. [ADO_IGS.1.2D-EXP3]	**X**
Content and presentation of evidence elements:	
The guidance documentation shall be complete, clear, consistent and reasonable. [AVA_MSU.1.2C]	**X**
The guidance documentation shall describe the functions and interfaces available to each of the authorized user types of the TOE. [AGD_ADM.1.1C, AGD_USR.1.1C - **refined**]	**X**
The guidance documentation shall describe the use of authorized user-accessible security functions provided by the TOE [AGD_USR.1.2C - **refined**]	**X**
The guidance documentation shall describe how to administer the TOE in a secure manner. [AGD_ADM.1.2C -**refined**]	**X**
The guidance documentation shall list all assumptions about the intended environment. [AVA_MSU.1.3C]	**X**
The guidance documentation shall contain warnings about functions and privileges that should be controlled in a secure processing environment. [AGD_ADM.1.3C, AGD_USR.1.3C - **refined**]	**X**
For each authorized user type, the guidance documentation shall clearly present all authorized user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding authorized user behavior found in the statement of TOE security environment. [AGD_ADM.1.4C, AGD_USR.1.4C - **refined**]	**X**
The guidance documentation shall describe all security parameters under the control of the authorized user, indicating secure values as appropriate. [AGD_ADM.1.5C - **refined**]	**X**
The guidance documentation shall describe each type of security-relevant event relative to the authorized user functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. [AGD_ADM.1.6C - **refined**]	**X**
The guidance documentation shall be consistent with all other documentation supplied for evaluation. [AGD_ADM.1.7C, AGD_USR.1.5C - **refined**]	**X**
The guidance documentation shall describe all security requirements for the IT environment that are relevant to each of the authorized user types. [AGD_ADM.1.8C, AGD_USR.1.6C- **refined**]	**X**
The guidance documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. [ADO_IGS.1.1C - **refined**]	**X**
The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences	**X**

Usage guidance documentation	AAL3
and implications for maintaining secure operation. [AVA_MSU.1.1C]	
The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls). [AVA_MSU.1.4C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	**X**
The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration. [ADO_IGS.1.2E]	**X**
The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation. [AVA_MSU.1.2E]	**X**
The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected. [AVA_MSU.1.3E]	**X**

A.7 Assurance through securing the development environment

A.7.1 Objectives

Development security is concerned with physical, procedural, personnel, and other security measures that may be used in the development environment to protect the TOE. It includes the physical security of the development location and any procedures used to select development staff. It is related to configuration management but deals more with the prevention of unauthorized access to the facility (ies) involved in the production of the monitoring equipment. This is important because an adversary might interfere with the production of the monitoring equipment, including the insertion of 'back-doors' or other weak points that could later be exploited in the operational environment

A.7.2 Application notes

The important thing is that the developer has suitable measures to protect the development environment. These need to be explained to the assessor in a way that they understand those measures and can ascertain that they are being used. DTRA may choose to impose these requirements via contractual means and not ask the assessor to rigorously verify its application.

Securing the development environment	AAL3
Developer Action Elements:	
The developer shall produce development security documentation. [ALC_DVS.1.1D]	**X**
Content and presentation of evidence elements:	
The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment. [ALC_DVS.1.1C]	**X**
The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE. [ALC_DVS.1.2C]	**X**

Securing the development environment	AAL3
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ALC_DVS.1.1E]	**X**
The evaluator shall confirm that the security measures are being applied. [ALC_DVS.1.2E]	**X**

A.8 Assurance through life cycle tools and techniques

A.8.1 Objectives

Assurance can be gained in the final implementation of the monitoring equipment via the establishment of adequate procedures, tools and techniques used to develop, analyze, implement and maintain that equipment. These are termed the overall 'life cycle model' in the requirements in the table below. Although the use of such a life cycle model does not guarantee that the resulting equipment will be without fault, it does give more assurance that faults were not introduced via sloppy processes.

A.8.2 Application notes

The CC defines a standardized life cycle model as one approved by a 'group of experts'. Therefore, any life cycle model approved by DTRA can meet this requirement. This approval can be gained through contractual negotiations and/or could be a model accepted through other standards bodies (e.g., CMM, ISO).

The CC presentation of these elements often causes confusion. They have therefore been reworded, and reordered, here but have the same intent as those words. Therefore they are marked as 'refined' not as 'explicitly-stated'. For instance, the CC states that tools includes techniques and therefore only addresses tools in ALC_TAT. That has been expanded here so that the developer can easily see that appropriate tools and techniques could be used. In addition, the CC only states that tools need to be documented, only implying that they must be used. That has been made explicit here to aid the developer in understanding what they must do.

In addition, the requirements have been reordered to be more in line with the CC paradigm of having a list of actions for the developer to take, the quality measures for those actions, and the list of how the evaluator confirms those actions. For instance, the CC had a developer action to document options chosen and that was reordered to be a content requirement on the documentation.

Life cycle tools and techniques	AAL3
Developer Action Elements:	
The developer shall establish a life cycle model to be used in the development of the TOE. [ALC_LCD.1.1D]	**X**
The developer shall provide life cycle definition documentation. [ALC_LCD.1.2D]	**X**
The developer shall measure the TOE development using the life cycle model. [ALC_LCD.3.3D]	**X**
The developer shall use development tools and techniques, as appropriate, in the production of the TOE. [ALC_TAT.1.1D – **refined**]	**X**
The developer shall use implementation standards, as appropriate, as part of their life cycle model for all parts of the TOE. [ALC_TAT.3.3D – **refined**]	**X**

Life cycle tools and techniques	AAL3
Content and presentation of evidence elements:	
The life cycle model shall provide for the necessary control over the development and maintenance of the TOE. [ALC_LCD.1.2C]	**X**
The life cycle model shall be measurable. [ALC_LCD.3.3D – **refined**]	**X**
The life cycle model shall be standardized. [ALC_LCD.3.3D – **refined**]	**X**
The life cycle definition documentation shall describe the model used to develop and maintain the TOE. [ALC_LCD.1.1C]	**X**
The life cycle definition documentation shall explain how the model is used to develop and maintain the TOE. [ALC_LCD.2.4C]	**X**
The life cycle definition documentation shall describe the measurable nature of the life cycle model, including details of the arithmetic parameters and/or metrics used to measure the TOE against the model. [ALC_LCD.3.1C - **refined**]	**X**
The life cycle definition documentation shall explain why the model was chosen. [ALC_LCD.2.3C]	**X**
The life cycle definition documentation shall explain how the model is used to develop and maintain the TOE. [ALC_LCD.2.4C]	**X**
The life cycle definition documentation shall demonstrate compliance with the standardized life cycle model. [ALC_LCD.2.5C]	**X**
The life cycle definition documentation shall provide the results of the measurements of the TOE development using the measurable life cycle model. [ALC_LCD.3.6C]	**X**
The life cycle definition documentation shall identify the development tools and techniques used for the TOE. [ALC_TAT.1.1D - **refined**]	**X**
The life cycle definition documentation shall describe the selected implementation-dependent options of the development tools. [ALC_TAT.1.2D - **refined**]	**X**
The life cycle definition documentation shall unambiguously define the meaning of all statements used by the tools and techniques in the implementation. [ALC_TAT.1.2C - **refined**]	**X**
The life cycle definition documentation shall unambiguously define the meaning of all implementation options used in the tools and techniques for the TOE. [ALC_TAT.1.3C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ALC_LCD.1.1E, ALC_TAT.1.1E]	**X**
The evaluator shall confirm that the implementation standards claimed have been applied. [ALC_LCD.3.2D – EXP, ALC_TAT.2.2E]	**X**

A.9 Testing

A.9.1 Objectives

Testing is used to establish that the functional requirements are met. Testing provides assurance that the monitoring equipment satisfies at least the monitoring equipment requirements, and includes both positive testing based on the functional requirements and negative testing to check that undesirable behavior is absent.

A.9.2 Developer Functionality Testing

A.9.2.1 Objectives

Testing the functionality is needed in order to demonstrate that all the monitoring equipment security functions perform as specified. The need is for sufficient testing to be performed and to provide sufficient test documentation to enable the testing performed to be understood. The assessment is achieved through an examination of the developer testing approach and a review of the results of the testing. The approach should show that the scope of the testing (i.e. coverage of the functions) and the level of abstraction of the testing (i.e. depth of the functional representation) were sufficient to adequately exercise the equipment's functions.

A.9.2.2 Application notes

The requirements for the contents of the test documentation are such that an assessor can determine that the approach taken was sound. This does not mean that a great deal of analysis needs to be provided in the documentation but rather must contain enough information so that the assessor can understand the approach sufficiently to make a judgment as to its sufficiency.

Testing the Functionality	**AAL3**
Developer Action Elements:	
The developer shall test the TSF and document the results. [ATE_FUN.1.1D]	**X**
The developer shall provide test documentation. [ATE_FUN.1.2D]	**X**
Content and presentation of evidence elements:	
The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. [ATE_FUN.1.1C]	**X**
The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed. [ATE_FUN.1.2C]	**X**
The test documentation shall describe test procedure ordering dependencies. [ATE_FUN.2.6C - **refined**]	**X**
The test documentation shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. [ATE_COV.1.1C - **refined**]	**X**
The test documentation shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete. [ATE_COV.2.2C - **refined**]	**X**
The test documentation shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design. [ATE_DPT.1.1C - **refined**]	**X**
The test documentation shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design, low-level design and implementation representation. [ATE_DPT.3.1C - **refined**]	**X**
The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. [ATE_FUN.1.3C]	**X**
The expected test results shall show the anticipated outputs from a successful execution of the tests. [ATE_FUN.1.4C]	**X**

Testing the Functionality	AAL3
The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. [ATE_FUN.1.5C]	X
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ATE_FUN.1.1E]	X

A.9.3 Independent Testing

A.9.3.1 Objectives

The aim is to independently demonstrate that the security functions perform as specified. Such assessor testing includes selecting and repeating a sample, or all, of the developer tests. It also includes independently developing and executing tests that may exercise the equipment in different ways than did the functional testing. However, the more thorough the developer testing, the more difficult it may be for the assessor to think of more testing techniques. Therefore, the assessor will need to make a judgment over the appropriate balance between repeating developer testing and performing new tests.

A.9.3.2 Application Notes

The following requirements call for the evaluator to perform the tests but do not specifically call for the way in which they plan or document those tests.

Independent Testing	AAL3
Developer Action Elements:	
The developer shall provide the TOE for testing. [ATE_IND.2.1D]	X
Content and presentation of evidence elements:	
The TOE shall be suitable for testing. [ATE_IND.2.1C]	X
The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. [ATE_IND.2.2C]	X
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [ATE_IND.2.1E]	X
The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified. [ATE_IND.2.2E]	X
The evaluator shall execute a sample of tests in the test documentation to verify the developer test results. [ATE_IND.2.3E]	X
The evaluator shall execute all tests in the test documentation to verify the developer test results. [ATE_IND.3.3E]	X

A.9.4 Strength of probabilistic functions

A.9.4.1 Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those

functions a qualification of their security behavior can be made using the results of a quantitative or statistical analysis of the security behavior of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.

Strength of TOE security function evaluation	**AAL3**
Developer Action Elements:	
The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim. [AVA_SOF.1.1D]	**X**
Content and presentation of evidence elements:	
For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST. [AVA_SOF.1.1C]	**X**
For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST. [AVA_SOF.1.2C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [AVA_SOF.1.1E]	**X**
The evaluator shall confirm that the strength claims are correct. [AVA_SOF.1.2E]	**X**

Identification of equipment vulnerabilities

A.9.4.2 Objectives

The assessor performs an analysis of the monitoring equipment to determine if vulnerabilities may exist. The assessor does this by using the results of all the assurance measures to postulate possible points at which the equipment might be compromised. The assessor then tests the equipment to determine whether those vulnerabilities exist. The developer should also take the possibility of equipment vulnerabilities into account when making design decisions in the development and implementation of the equipment. They therefore should provide some evidence that vulnerabilities have been considered and how they have been eliminated, minimized, or made to be detectable.

A.9.4.3 Application Notes

The vulnerability identification for DTRA monitoring equipment is, by its nature, different than that expected in the CC. The CC assumes a type of threat environment and requires that any vulnerability that exists in that environment be eliminated. Monitoring equipment is placed in an extremely high threat environment and needs to know when the equipment is compromised, not necessarily to prevent the compromise from happening. This is because the cost for developers to provide functionality to prevent such compromises is too high for DTRA to bear (and for host supply equipment, this is an unrealistic approach). However, they will require some level of compromise to be prevented and can provide a list of those as input to the assessment process. This list is represented as an ‘assignment operation’ to be filled in for a given equipment assessment.

In addition, the amount of analysis and testing performed by the assessor in looking for and demonstrating potential vulnerabilities is also a cost factor. Therefore, DTRA will provide a list of

vulnerability types to take into account in the assessment and will provide a degree of effort that the assessor is expected to undertake in identifying potential vulnerabilities beyond that list.

Vulnerability analysis	**AAL3**
Developer Action Elements:	
The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP. [AVA_VLA.2.1D]	**X**
The developer shall document the disposition of identified vulnerabilities. [AVA_VLA.2.2D]	**X**
Content and presentation of evidence elements:	
The documentation shall describe the methods used to identify TOE vulnerabilities. [AVA_VLA.2.xC - EXP]	**X**
The documentation shall describe the measures taken to address the identified vulnerabilities, including the degree to which each has been eliminated, minimized or made to be detectable. [AVA_VLA.2.1C - EXP]	**X**
The documentation shall justify that the TOE is resistant to [assignment: DTRA defined list of] penetration attacks. [AVA_VLA.2.2C - EXP]	**X**
The documentation shall show that the search for vulnerabilities is systematic. [AVA_VLA.3.3C]	**X**
The documentation shall justify that the analysis completely addresses the TOE deliverables. [AVA_VLA.4.4C]	**X**
Evaluator action elements:	
The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. [AVA_VLA.1.1E]	**X**
The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure identified vulnerabilities have been addressed. [AVA_VLA.1.2E]	**X**
The evaluator shall perform an independent vulnerability analysis to the rigor [assignment: degree of DTRA-defined rigor]. [AVA_VLA.2.3E - **refined**]	**X**
The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the DTRA monitoring environment. [AVA_VLA.2.4E - **refined**]	**X**
The evaluator shall determine the degree of resistance of the TOE to penetration attacks based on [assignment: DTRA list of vulnerability types]. [AVA_VLA.2.5E - EXP]	**X**

B ANNEX: OPERATIONAL ASSURANCE

B.1 DTRA Requirements

The DTRA will be acting in several roles for the assessment of the ISMS and future monitoring systems. The subset of the responsibilities within these roles impacting the technical efficacy of the assessment is as follows:

- B.1.1 Set the requirements for the developer of the equipment.
- B.1.2 Agree the level of threat to be addressed by the combination of deployed equipment.
- B.1.3 Agree the appropriate AAL to be applied to a specific equipment.
- B.1.4 Provide the appropriate equipment to perform the monitoring function.
- B.1.5 Provide the appropriate information to technicians installing and maintaining the equipment.
- B.1.6 Provide the appropriate information to inspectors for determining that the equipment remains secure during its operation.
- B.1.7 Provide appropriate infrastructure for handling monitoring information appropriately,.
- B.1.8 Set standards for the technical expertise, independence and working methods of assessors.
- B.1.9 Provide configuration information for equipment, either in lieu of or in supplement to developer information.

Although these requirements could be expressed in [CC] terms, they are not the focus of this paper. However, DTRA will need to ensure that these requirements are included in the overall monitoring process and procedures.