PNNL-13743

A Review of the IAEA Vulnerability Assessment Level Scheme:
Applicability to DTRA and DOE Programs in the FSU[1]

M. DeVaney, R. Hansen, R. Kouzes, and R. Melton

Version 1.0

12 December 2001

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 Inventory Sampling 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)

Abstract

The International Atomic Energy Agency (IAEA) plans to use the ISO standard Common Criteria (CC) as the tool for developing graded and measurable evaluation criteria for information technology in safeguards systems in facilities subject to IAEA inspection. This paper reviews the IAEA approach to use of the CC standard and makes comparisons to the possible use of the CC standard by US agencies.

Table of Contents

1. Introduction

The information technology community has created a standard called the Common Criteria for Information Technology Security Evaluation ("Common Criteria", or "CC") [CC]. The CC is a catalog of criteria and a framework for organizing a subset of the criteria into security specifications and evaluation specifications. The CC defines a set of "Evaluation Assurance Levels" (EALs) that are a set of selected criteria for evaluation of information technology security. The EAL concept can be extended to define levels of authentication, and the associate procedures to reach these levels, with regard to a Target of Evaluation (TOE). Evaluation has been the traditional means of gaining assurance, and is the basis of the Common Criteria approach.

The IAEA plans to use the Common Criteria, as the tool for developing graded and measurable evaluation criteria for information technology (IT) in safeguards systems in facilities subject to IAEA inspection. In their draft paper [ITSECSES] the IAEA defines a three-tiered Vulnerability Assessment Level (VAL) scheme. Each increased VAL level (1-3) defines additional and more stringent security and security-related requirements for the system developer, the system evaluator (assessor or authenticator), and for the IAEA. When all parties meet all requirements for a particular VAL level, the IAEA has a measurable degree of confidence in the secure and proper operation of an IT system.

In [ITSECSES] the IAEA only addresses the security evaluation or assessment of IT and does not specify security requirements per-se. However, the paper does recommend the development of CC Protection Profiles (information security requirements in CC parlance) for specific purpose IT and for the use of previously evaluated products for commonly available commercial off-the-shelf IT components (e.g., general-purpose operating systems, database management systems, and firewalls).

Independent of the IAEA effort, the Russian Federation (RF) is taking steps to adopt the Common Criteria as a Russian Standard and to enter the Common Criteria Recognition Arrangement [CCRA]. They are being aided in this effort through the United States Department of Energy (DOE) Nuclear Material Protection, Control, and Accounting (MPC&A) Program. Successful completion of these actions will facilitate RF meeting its information security requirements with respect to non-domestic IT used (increasingly) in safeguards systems and elsewhere. Adoption of CC should also make it relatively easy for the RF to step up to other CC-derived requirements, such as the IAEA plan we review here.

The Defense Threat Reduction Agency (DTRA) and DOE also need to establish confidence in the proper and secure functioning of IT systems in the states of the Former Soviet Union (FSU), especially in the Russian Federation.[2] DTRA must authenticate systems used to safeguard FSU weapon-origin nuclear material. DOE has (possibly less stringent) assurance requirements for IT systems used to safeguard FSU weapons-grade nuclear material. The US has adopted the Common Criteria for information technology

[2] PNNL is developing authentication methodology for the FMSF under contract to DTRA.

security evaluation and is a signatory to [CCRA]. Given the RF intent to adopt the CC, an approach similar to that in [ITSECSES] has potential to satisfy DTRA and DOE authentication/assurance requirements.

2 Notes on RF IT Security Practices

In reviewing [ITSECSES] definition of the VALs with a view to implementing a similar approach to evaluating/authenticating IT systems in the RF, certain issues need to be raised. There are two well-entrenched concepts in RF approach to IT systems that make proper application of the CC a challenge. First, in their approach to security, in the RF a security evaluation does not set out to manage risk, but to guarantee it has been eliminated. The North American and Western European information security community has reached a strong consensus that one must deal with uncertainty and manage security risks that cannot be completely eradicated. Second, in the RF approach to the system development and life cycle for IT, one does not plan to manage change (e.g., in specifications or system design). In the RF, when one accepts specifications, design, and implementation one guarantees the perfection (now and into the future) of these levels of abstraction of an IT system. As a result there is a strong incentive for both developer and customer to create lots of wiggle room in specifications, design documents, etc., so that when the inevitable problems arise, the system (at any level of abstraction) can still be said to meet all requirements.

The former issue has made translation of [CC] into the Russian language a very difficult endeavor at times. The issue of not sharing the same understanding of the management of risk and uncertainty in IT security evaluation may seriously delay RF accession to the CCRA – it is that important to the members of the CCRA (and membership requires unanimous approval of all 14 members[3]). Anyone discussing information security evaluation issues with representatives of the RF needs to bear in mind these fundamentally different approaches to IT between our cultures.

The latter issue occasionally makes contracting for the development of IT in the FSU a challenge for North Americans and Western Europeans – it's hard to pin them down. In Section 2.4.2 [ITSECSES], the IAEA cites ISO standards for Life Cycle Management as good examples of standards with which they could agree. These are standards that may be difficult for the RF to step up to, much less adopt in the near future. That said, the IAEA recommends an approach to life cycle management that may fit the RF situation (Annex A.7.2 [ITSECSES]):

> "The CC defines a standardized life cycle model as one approved by a 'group of experts'. Therefore, any life cycle model approved by the IAEA 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)."

Since to be effective this approach requires agreeing to a specific life cycle plan, those who need to define the maintenance of assurance (authentication) throughout the life cycle of IT must plan to put considerable effort into negotiating this bit. DTRA and DOE might do well to promote either adoption by RF of a recognized life cycle management standard or to negotiate this issue on a global basis for their Programs.

[3] Members of the CCRA include: Australia, Canada, Finland, France, Germany, Greece, Italy, Israel, Netherlands, New Zealand, Norway, Spain, United Kingdom, and United States.

On a positive note, the information security elements of the Ministry of Atomic Energy of the Russian Federation are indicating interest in certifying a family of open source GNU/Linux operating systems. This could provide RF a foundation on which they could develop everything from embedded systems for measurement instruments and physical protection equipment to large (e.g., multi-CPU, multi-tier servers) management system applications. With source code available they can:

- Modify GNU/Linux to meet RF's stringent information security requirements.
- Meet typical assurance levels expected of general purpose operating systems as may be required by the IAEA, DTRA, DOE, and others.
- Meet strong assurance levels for a small critical equipment by minimizing the features of an embedded GNU/Linux operating system.

3 Authentication Variation Between the IAEA and the U.S. Government

The IAEA goal with inspection and monitoring activities is to verify that nuclear material under agreement is as declared and that it remains in place. IAEA monitoring employs on-site inspections, on-site monitoring, and remote monitoring. On site material is randomly sampled for the IAEA to conduct non-destructive assay (NDA) measurements and accounting records and procedures are reviewed. Remote monitoring via video surveillance cameras utilizing a combination of motion video and still images reduces the cost of monitoring. Images and video may be shipped to the IAEA or reviewed on site during monitoring visits. The IAEA supplies evaluated equipment for NDA testing and video surveillance. The IAEA conducts (through qualified contractors) evaluation of equipment (it's trusted). The IAEA has strong control of the NDA equipment they use on-site. The IAEA's main problem with respect to the on-site equipment is to protect the integrity of their evaluated equipment. The IAEA is concerned the monitored facility may be able to spoof their trusted equipment.

Although the goal of inspection and monitoring activities is highly similar, there are key differences between DTRA's compliance monitoring scheme at the Fissile Material Storage Facility and the IAEA approach briefly discussed above. These are mostly driven by national security concerns of the Russian Federation. DTRA monitors will not operate the NDA equipment. The host country (Russia) will supply the monitoring equipment. The host country will operate the monitoring equipment. The host country will conduct security evaluations of the monitoring equipment, after which DTRA representatives will no longer be allowed to touch the equipment. DTRA will have relatively strong control of the Inventory Sampling Measurement System, but this is much less so for the other monitoring equipment at the Fissile Material Storage Facility. It is likely that review of video surveillance imagery will be available only on-site. DTRA's main problem with respect to the on-site monitoring equipment is that the equipment cannot be trusted. DTRA must continually attempt to re-authenticate the monitoring equipment without touching it. DTRA is concerned the monitoring equipment itself contains flaws that prevent accurate measurements and monitoring.

4 Defines IAEA Assurance Requirements

The IAEA defines assurance requirements only. The differences between security functions and assurances are made clear in Section 3 [ITSECSES]. There is no mistaking that this document does not specify security functions/requirements. In Strategies to Minimize Evaluation/Assessment Costs (Section 5 [ITSECSES]) the IAEA calls for the separate Creation of IAEA Standard Protection Profiles (Section 5.3 [ITSECSES]).

It is clear the IAEA is in tune with the CC understanding of information security assurance. In Section 3.1.2 [ITSECSES] it is made clear that assurance is gained through both technical and procedural means – a holistic view of IT systems. The necessity to identify and manage risk is discussed. It is recognized that exorbitant cost may be required to completely eliminate a risk and it may be necessary to modify the system to minimize the impact of exposure to that risk. Further it is advocated that for some risks the system can be monitored to detect occurrences of compromise and that mitigation of the detected compromise may be the appropriate cost-effective remedy.

The IAEA maps the life cycle for IT to their existing framework for the authorization of Equipment Systems and Application Software for safeguards use and also to the CC approach (Section 3.2 [ITSECSES]). The mappings demonstrate there are no missing elements for the IAEA in adopting the CC approach.

The CC deals with assessment issues and requests for clarifications from the developer by defining Observation Reports (OR) in the companion document Common Evaluation Methodology [CEM]. The Evaluation Technical Report (ETR) is defined in [CEM] to document the technical justification for the assessment verdict. OR and ETR reports can be made to satisfy IAEA requirements for standardized documentation of assurance for various equipments (Section 3.2 [ITSECSES].

5 Roles in the Context of Assurances

Five roles are defined [ITSECSES] in the context of assurances:

- IAEA Oversight
- Safeguards Equipment Developers
- Vulnerability Assessors
- Inspectors
- Operational Users.

The first four of these are assigned responsibilities to implement specific assurance criteria. The operational users, on the one hand, are part of the environment and threat, and on the other hand, their proper use of the equipment drives certain assurance criteria (e.g., user interface clarity, simplicity, and consistency) and documentation criteria (e.g., user guide documentation quality). Inspectors (IAEA personnel) have responsibilities to monitor ongoing assurance indicators and perform maintenance of assurance checks/procedures during periodic inspection visits.

These roles are reasonably consistent with DTRA and DOE practice with respect to IT projects in the FSU. However, there are minor differences in terminology and function. DTRA would use Authentication Assessors in place of Vulnerability Assessors and Monitors in place of Inspectors. Under the DOE MPC&A Program, formal information security assurances are not required and less formal IT system acceptance criteria are substituted. DOE Project Managers accept contracted MPC&A IT systems on technical requirements negotiated into each development contract. The MPC&A program does not include an ongoing oversight function, and thus there is no monitor role.

6 The IAEA Vulnerability Assessment Levels (VAL)

In [ITSECSES] the IAEA discusses CC concepts for assurance and describes the eight CC assurance classes:

ACM Control over the configuration of the equipment
ADO Confidence the Equipment was the One Shipped and it is Installed Correctly
ADV Confidence Through the Process of Development
AGD Documentation Delivered with the Equipment
ALC Assurance Gained Throughout the Product Life Cycle
ATE Testing
AVA Determination of System Vulnerabilities
AMA Maintenance of Assurance After Assessment

For each of these classes typical high-level requirements are called out for the roles defined above (excepting the operational users). These high-level requirements are not the specific assurance criteria – these are defined in [ITSECSES] in Annex A (Safeguards Equipment Developers), Annex B (Vulnerability Assessors), and Annex C (IAEA Oversight and Inspectors (including technicians)).

The IAEA is in agreement with these CC classes, which are further broken down into families (two to seven per class) of related requirements in the CC documentation, where specific criteria are spelled out. [CC3] provides some 208 pages of detailed individual criteria in these classes and families.

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 - semi formally designed and tested
- EAL6 - semi formally verified design and tested
- EAL7 - formally verified design and tested

The IAEA elected not to use any of the predefined packages, but instead identified three of their own, which they have identified as Vulnerability Assessment Levels (VALs). The IAEA defined the packages they needed to provide a balance between a reasonable and appropriate combination of threats to the equipment in the safeguards environment and budgetary considerations. This custom package declaration is acceptable and expected practice under the CC.

The VALs are assembled such that they roughly correspond to EAL3, EAL4, and EAL5 – but they are not identical to these. The VALs increase in strength from VAL1 through VAL3. Their names provide good indicators of their intended applicability:

- VAL1 Minimally Acceptable Assessment

- VAL2 State of the Art Assessment
- VAL3 Critical Equipment Assessment

VAL1 “is meant to be used to assess the vulnerabilities of equipment supporting overall safeguards operation but not containing safeguards critical information. It is a statement of the minimal assurance expected of commercial-off-the-shelf equipment.” This is a not unreasonable position for the IAEA to take and this is borne out by reviewing the large number of CC evaluated products that have met or are being targeted at EAL3 and EAL4. Even if the IAEA would permit host built equipment, VAL1 would probably be difficult to achieve by host country developers in some of the less well-developed countries under IAEA safeguards inspection.

VAL2 “encapsulates the package of assurance measures that the IT market expects of commercial-off-the-shelf equipment protecting sensitive information. It is the preferred assurance that any equipment used in nuclear safeguards should have.” It is not unreasonable for the IAEA to target this level as many completed and in process CC evaluations are targeted at level EAL4. Although commercial off-the-shelf components already evaluated at EAL4 will not fully meet VAL2, there are positives here. First, in some cases the developer may be able to meet VAL2 with a minimum of effort starting with an EAL4 component and layering additional security features. Second, the regularity with which EAL4 is being targeted is a strong indicator that good developer practice can result in achieving VAL2 at reasonable cost.

VAL3 “encapsulates the level of assurance economically possible for equipment used in nuclear safeguards. It encapsulates the security processes and procedures shown to provide substantial added assurance in the security features of equipment.” With this level, the IAEA calls out several criteria that are quite demanding of the developer. Appropriately, they note that VAL3 is intended for small, critical, specialty equipment, and they expect that in order for such equipment to meet VAL3 will add a relatively large cost to equipment development.

7 Cost Containment

A number of practical measures are proposed to contain costs in an IAEA evaluated products environment:

- Use of Standard Assessment Processes
- Early Integration of Security Requirements into Project Planning
- Creation of IAEA Standard Protection Profile(s)
- Early Input to Functional Design
- Role of Pre-Evaluated Products.

All of these are sensible recommendation that we endorse. In ANNEX E [ITSECSES], the IAEA recommends the use of industry standard information security profiles wherever possible to specify the appropriate security functionality for safeguards equipment. They recommend defining specialized IAEA requirements for as few components as possible. This seems a wise strategy for managing both cost and schedule.

8 Selected Criteria

A summary of the selected criteria, newly defined criteria, and revised criteria, defined in Annex A [ITSECSES] is presented in Table 1 below.

CC class	Description	Criteria count	New	Revised
ACM	Control over the configuration of the equipment	24	0	0
ADO	Confidence the Equipment was the One Shipped and it is Installed Correctly	6	1	0
ADV	Confidence Through the Process of Development	77	0	0
AGD	Documentation Delivered with the Equipment	26	1	11
ALC	Assurance Gained Throughout the Product Life Cycle	21	0	8
ATE	Testing	25	0	5
AVA	Determination of System Vulnerabilities	12	0	2
AMA	Maintenance of Assurance After Assessment	52	0	0
	TOTALS	**243**	**2**	**26**

Table 1: Selected Criteria

Analysis of the selected criteria indicates strong IAEA interest in customizing the assurance classes for documentation (AGD) and life cycle (ALC), and moderate interest in customizing the assurance classes for testing (ATE) and determination of system vulnerabilities (AVA). For documentation class AGD, many of the changes seem to be driven by two IAEA concerns (inferred from analyzing the differences between the revised and original criteria):

- Documentation should be provided by role (administrator, user, etc).
- Documentation should be organized in an IAEA standard manner.

These issues dominate the revisions in the documentation class. This may well be an important issue for the IAEA, but to the extent it inhibits re-use of CC certified evaluations of general purpose components, it may not be a good direction for others to take.

For the life cycle class (ALC), the revisions are acknowledged by the IAEA as minor, but were made in an attempt to make these requirements more explicit and clearly understandable to developers. Given the IAEA emphasis on life cycle (especially during

equipment operational lifetime) this is understandable, but again to the extent it inhibits re-use of CC certified evaluations of general purpose components, it may not be a good direction for others to take.

The number of criteria specified for development class ADV is not remarkable. This is an important area and has the greatest number of families (subclasses) of criteria (seven) of any CC class. It is perhaps interesting that none of these are revised in [ITSECSES]. This may be more a case of the keen attention paid this class by the authors of the CC than to any lack of interest by the IAEA.

Maintenance of assurance after assessment (AMA) is an interesting class in that the authors of the CC have acknowledged their general dissatisfaction with what they have so far produced. Significant changes are planned for the next version of the CC due in draft form in fall, 2001 and likely adoption in the second half of CY 2002. Maintenance of assurance is a stated interest area for the IAEA and this interest is reflected in the number of criteria selected. Given the relative immaturity of these criteria in the CC, it seems remarkable that the IAEA had no new criteria and no revisions in this class. One surmises the IAEA is aware of coming changes to the CC and is merely biding their time in this area. In other words, despite the number of criteria selected, this may be a placeholder.

9 Other Assurance Roles

9.1 Assessor (Authenticator) Assurance

The IAEA defines a reasonable set of "… requirements on assessors in the handling of assessment information and the reporting requirements to the IAEA" (ANNEX B [ITSECSES]). This is an important addition since the IAEA intends to do their own evaluations and may not be using testing laboratories certified under any country's National Scheme for CC evaluations. This approach may well apply to DTRA and DOE authentications and assurances for IT monitored in the FSU. The criteria in this section (ANNEX B) are all newly defined criteria. The criteria are based on an interpretation of guidance and recommendations provided in [CEM2], a companion document to [CC] that is not part of the ISO standard.

Criteria are defined to manage the assessor's assessment reports and associated materials and documentation. Criteria are defined to assure safe and sound delivery of an IAEA Vulnerability Assessment Technical Report (IAVATR). Criteria are defined to govern the preparation and content of the IAVATR, modeled after the CC Evaluation Technical Report (ETR). It is made clear that the IAVATR is not a pass/fail determination, but a detailed report of "… how well the equipment has stood up to the specific attack scenarios provided as input to the assessment. In particular, the assessor must confirm that the implementation of the functional requirements clearly meets the statements of which threats have to be eliminated, minimized or monitored."

Criteria are defined to assure the assessment test tools and methods are appropriate. Finally, criteria are defined to assure the assessment testing is appropriate. These last two sets of criteria are partly an attempt to step up to the problem that the IAEA so far has no certification program for assessors and assessment laboratories.

In Vulnerability Assessors (Section 3.3.3 [ITSECSES]), the IAEA addresses the certification criteria (qualifications) for assessors and assessment laboratories and certification criteria for evaluators and evaluation laboratories through its member states:

> "The IAEA generally receives vulnerability assessments on safeguards equipment systems via Member State experts who follow a general set of assessment criteria prepared by the Agency. These assessments would be based on the [CC] and [CEM] in order to ensure comparable results. As many Member State experts move toward the use of third-party laboratories, the IAEA will also have access to these resources. Under the Common Criteria Recognition Arrangement (CCRA), these laboratories are subject to strict quality standards ([EN45000] and [ISO17025]). In addition, the national oversight of these laboratories (and international CCRA oversight) further assures technical competence."

It would also be interesting to review the Common Criteria National Scheme for one or more of the CCRA members to see how security evaluator qualifications and certification is addressed.

9.2 IAEA Oversight and Inspector Assurances

In ANNEX C [ITSECSES], the IAEA sets forth criteria that apply to the roles for IAEA Oversight and Inspectors (including technicians). The discussion is limited to the scope these roles play in Vulnerability Assurance.

Among the criteria set forth for IAEA Oversight is to "Set standards for the technical expertise, independence and working methods of assessors." One could infer from this that the IAEA will set criteria for assessors on a case-by-case basis, but this would put at risk their goal of establishing an inventory of pre-assessed equipment that could be used for new installations/systems. Although not discussed in [ITSECSES] one presumes that the IAEA plans to set requirements for assessors on a global (not product) basis and provide for updates and waivers to those requirements.

10 Other Issues

10.1 IAEA Procedures

In ANNEX D [ITSECSES], the IAEA provides a brief discussion of related internal issues. The IAEA requires integrating this proposed assurance scheme into their existing procedures for authorizing safeguards equipment.

10.2 Integration of Security Requirements into Product Life Cycle

As IAEA security requirements extend into the operational life of equipment, this section of ANNEX D provides a general discussion of standards for IT Life Cycle management in an international setting. [ITSECSES] notes that security requirements must be integrated into the product and associated procedures throughout the life of the equipment and software:

> "To meet security **functional** requirements, these requirements must be identified early, implemented during development, tested, and maintained during use.
>
> To meet security **assessment** requirements, assessment procedures (e.g. the development of documentation, evidence) must be integrated throughout the product definition, development, maintenance and operation."

Although the IAEA recognizes the need to address security functional requirements, in [ITSECSES] only security assessment requirements are discussed in detail.

10.3 International Standards for Life Cycle Processes

International standards for life cycle processes are discussed. It is noted that "… [ISO15288] is expected to be adopted internationally as the basis for system life cycle standardization." [ISO15288] is a high-level standard that does not mandate particular activities, but rather defines the processes required and provides a language that in conjunction with other (more detailed and more specific) standards defines project life cycles that implement these processes. It seems appropriate for the IAEA in an international setting to find [ISO15288] applicable. The section goes on to discuss good candidates for these more specific life cycle standards, in particular [ISO12207] and [IEEE12207.1] and [IEEE12207.2]. There are three classes of life cycle processes defined in [ISO12207], primary, supporting, and organizational processes. These are further broken down into five, eight, and four subclasses respectively. It is worth noting the names of the subclasses:

Primary Processes	Acquisition Supply Development Operation Maintenance
Supporting Processes	Documentation

	Configuration management Quality assurance Verification Validation Joint review Audit Problem resolution
Organizational Processes	Management Infrastructure Improvement Training

Table 2 – IEC/ISO 12207 Life Cycle Processes

It may be possible for the states of the FSU (especially RF) to adopt [ISO15288] and [ISO12207], and to develop standards equivalent to the [IEEE12207] family. Realistically this would almost certainly require support from an interested outside entity (e.g., DTRA, or DOE). This support would not only have to cover the technical aspects of translation and submission through internal adoption mechanisms, but education of staff in appropriate technical organizations. Experience contracting for RF software development projects under the MPC&A Program indicates there are existing but generally outmoded standards for most if not all of the subclasses for Primary and Organizational Processes defined in [ISO12207]. However, the same experience indicates a severe shortfall in current RF standards concerning most if not all of the defined subclasses for the Supporting Processes above.

As an example of the shortfall in standards and the associated education problem, the quality assurance subclass above is potentially an important aspect of security assurance. Indeed in ANNEX D [ITSECSES] it is discussed and there is mention of the Software Engineering Institute's integrated Capability Maturity Model [CMMI]. The IAEA is already interested in EAL5 and one would anticipate eventual IAEA interest in EAL6 and possibly EAL7. EAL5 and EAL6 require semiformal methods and EAL7 requires formal methods of system development. [CMMI] addresses both semiformal and formal methods. Again adoption in the RF of [CMMI] or any other semiformal and formal methods standard would almost certainly require support including education from an interested outside entity (e.g., DTRA, or DOE).

10.4 Safeguards Functionality for Remote Monitoring

The bulk of ANNEX E [ITSECSES] is concerned with aspects of remotely monitoring safeguards equipment. This requires a discussion of cryptography algorithms and protocols, encryption key management, authentication of data collected during remote monitoring, and transmission security among other issues. This falls outside our current scope of interest.

11 Summary

The line of reasoning followed in [ITSECSES] is largely applicable to DTRA and DOE authentication and assurance requirements for IT used to monitor and manage weapons origin and weapons grade nuclear material. There are enough differences in the underlying missions and the relationship with the nuclear states being monitored that it is not realistic for these agencies to adopt the IAEA approach as is. However, significant portions of the IAEA approach provide a good model for what is needed by DTRA and DOE. In the future, it seems possible that the IAEA, DTRA, and DOE might be able to recognize and use one another's evaluations of specialized safeguards equipment, in much the same way that [CCRA] is intended to work.

However, agencies like DTRA and DOE need to evaluate the specific threats in their respective mission environments and develop a set of specialized Authentication Assurance Level (AAL) packages for those cases where they will require unique protection profiles. On the basis of threat evaluation for a specific situation DTRA and DOE should select pre-evaluated products and use existing protection profiles and assurance level packages (from Common Criteria and possibly from the IAEA) where these will satisfy the functional security requirements and assurance requirements. On occasion, DTRA and DOE will need to develop unique protection profiles for specialized equipment and employ their AALs when evaluating these products.

For the RF to be able to step up to developing systems with functional security requirements and security assurance requirements at AALs approximating EAL5 and above, it will be necessary to support them in adopting standards equivalent to [ISO15288], [ISO12207], and [CMMI]. An effort to educate (selected elements in) the RF to use the associated tools and methods will almost certainly also be required. This is a natural progression from support they have received thus far toward the adoption of the [CC] and [CCRA]. It may even prove difficult to consistently achieve an AAL approximating EAL4 without these standards and education investments.

12 Path Forward, DTRA Authentication with AALs

In developing a set of draft AALs with which to authenticate the Inventory Sampling Measurement System and possibly other monitoring equipment at the Mayak FMSF, PNNL has defined five Authentication Assurance levels, briefly described below:

AAL0 Unauthenticated
: Equipment that has not received any assessment relative to authentication.

AAL1 Minimally Authenticated
: This AAL encapsulated the minimum level of assurance that any equipment used in nuclear safeguards should have. It encapsulates the security processes and procedures generally employed in the information technology industry to obtain a basic understanding of the equipment's functionality and potential vulnerabilities.

AAL2 Limited Authentication
: This AAL encapsulates the package of assurance measures that the IT market expects of commercial-off-the-shelf equipment protecting sensitive information.

AAL3 Critical Authentication
: This AAL encapsulates the level of assurance economically realizable for equipment used in nuclear safeguards. It encapsulates the security processes and procedures shown to provide substantial added assurance in the security features of equipment. It is the preferred assurance that any equipment used in nuclear safeguards should have.

AAL4 Optimal Authentication
: This AAL encapsulates the maximum level of assurance economically possible for equipment used in nuclear safeguards. It encapsulates the security processes and procedures shown to provide substantial added assurance in the security features of systems.

AAL3 is considered as a reasonable target Authentication Assurance Level for monitoring equipment, and is described in detail in [PNNL]. Because the Russian Federation has yet to adopt the CC (though there is an active effort underway to do so) PNNL has developed guidance material to assist the monitoring equipment developers to meet the appropriate target AAL. A sample from the current working version of this guidance is provided in the following tables.

	AAL1	AAL2	AAL3	AAL4
Configuration Management (CM)	Consumer should have a way to identify that they have the version authenticated.	Consumer should have a way to identify that they have the version authenticated. The developer should use a CM system in the production of the equipment	Consumer should have a way to identify that they have the version authenticated. The developer should use a CM system in the production of the equipment The CM system should include a CM Plan describing how the CM system in used. The CM system should cover all development materials. The CM system should assure that only authorized changes are made	Consumer should have a way to identify that they have the version authenticated. The developer should use an automated CM system in the production of the equipment The CM system should include a CM Plan describing how the CM system in used. The CM system should cover all development materials and track security flaws The automated CM system should assure that only authorized changes are made
Delivery Procedures	Users should know how to install the equipment	Users should know how they will receive the equipment Users should know how to install the equipment	Users should know how they will receive the equipment Users should know how to install the equipment	Users should know how they will receive the equipment Users should be able to detect if the equipment has been tampered with during delivery Users should know how to install the equipment

	AAL1	AAL2	AAL3	AAL4
Development Processes	User should have an explanation of how to interface with the equipment	User should have an explanation of how to interface with the equipment Evaluators should understand the basic architecture of the equipment.	User should have an explanation of how to interface with the equipment Evaluators should understand the basic how architecture of the equipment, including the internal interfaces between the subsystems	User should have a comprehensive explanation of how to interface with the equipment Evaluators should understand the overall system security policies implemented in the equipment Evaluators should understand the basic how architecture of the equipment, including the internal interfaces between the subsystems Evaluators should understand the design to the level of subsystem modules. Evaluators should inspect a sample of the source code (or equivalent) to determine that it reflects the design
Guidance Documentation	Users and administrators need an explanation of security information relevant to them	Users and administrators need an explanation of security information relevant to them	Users and administrators need an explanation of security information relevant to them	Users and administrators need an explanation of security information relevant to them

	AAL1	EAL2	AAL3	AAL4
Life Cycle Support			The developer should take measures to secure the development facility	The developer should take measures to secure the development facility The developer should follow a life cycle model in the development of the equipment Any tools that the developer uses in the development of the equipment should be well defined and understood.
Testing	An independent evaluator should functionally test based on the interface definition	The developer should functionally test the equipment based on the interface definition The developer should conduct this testing according to test plans and procedures and document the results of the testing. An independent evaluator should functionally test based on the interface definition An independent evaluator should rerun a selection of the developer tests.	The developer should functionally test the equipment based on the interface definition The developer should conduct this testing according to test plans and procedures and document the results of the testing. An independent evaluator should functionally test based on the interface definition An independent evaluator should rerun a selection of the developer tests.	The developer should functionally test the equipment based on the interface definition The developer should conduct this testing according to test plans and procedures and document the results of the testing. An independent evaluator should functionally test based on the interface definition An independent evaluator should rerun a selection of the developer tests.

	AAL1	AAL2	AAL3	AAL4
Vulnerability Assessment		Any probabilistic mechanism should be strong enough to resist direct attack The evaluator should determine that the equipment resists known attacks	The user documentation should be clear so the user and administrator knows when the equipment is in a secure configuration. Any probabilistic mechanism should be strong enough to resist direct attack The evaluator should determine that the equipment resists known attacks	The user documentation should be clear so the user and administrator knows when the equipment is in a secure configuration. Any probabilistic mechanism should be strong enough to resist direct attack The evaluator should determine that the equipment resists attacks by personnel with some motivation and resource.

13 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).

[ITSECSES] Working Document for IT Security Evaluation Criteria for Safeguards Equipment Systems, International Atomic Energy Agency, Vienna, Austria (Version 2.0, 31 May 2001).

[PNNL] Authentication Assurance Level Application to the Inventory Sampling Measurement System, PNNL-13637, August, 2001