WIND RIVER

Security FAQs

Table of Contents

Q. What is 8500.1?

A. Dated October 24, 2002, **8500.1** is a Department of Defense (DoD) Directive on Information Assurance (IA) that states:

1. All IA or IA-enabled products incorporated into DoD IA systems *must* comply with NSTISSP 11
2. Products must be satisfactorily evaluated prior to purchase
3. Purchase contracts shall specify that product evaluation will be maintained for subsequent releases

See http://west.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf for a complete copy of this directive.

Q. What is 8500.2?

A. Dated February 12, 2003, **8500.2** is a DoD Instruction for Information Assurance Implementation that states:

1. If a Protection Profile (PP) exists for a specific technology, then products must be evaluated against this PP
2. A robustness level will be assigned—medium or high—which must be achieved

See www.dtic.mil/whs/directives/corres/pdf/850002p.pdf for a complete copy of this DoD instruction.

Q. What is ACTS?

A. **ACTS** stands for **A**dvanced Extremely High-Frequency **C**OM-SEC/**T**RANSEC **S**ystem. ACTS systems are usually involved in highly secure military command and control systems, like missile and satellite weapons systems.

Q. What is AR 25-2?

A. Dated November 14, 2003, **AR 25-2** is the Army Regulation 25-2 that establishes an IA policy for the Army. This regulation:

1. Specifies and defines roles and responsibilities. The Chief Information Officer, level G-6 (CIO/G-6) is the person responsible for execution of this regulation
2. Is implemented by Army Certification Authorities (two) and Combined Test Support Facility (Ft. Hood, TX)
3. Has general applicability to a broad range of technology: IT, water, power, and other infrastructure
4. Incorporates 8500.1 and 8500.2 for software IA

See www.army.mil/usapa/epubs/pdf/r25_2.pdf for more information.

Q. What is Assurance?

A. **Assurance** is the confidence (medium or high) that a component or system will meet security objectives.

Q. What is CCEVS?

A. **CCEVS** stands for Common Criteria Evaluation and Validation Scheme. This scheme:

1. Tests Security Properties of COTS products—these tests are performed by Accredited Commercial Laboratories
2. Validates the results underwritten by NIAP—these results are posted for public access

CCEVS is, in effect, the U.S. Government version of the Common Criteria for certification of critical systems at high EAL.

See http://niap.bahialab.com/cc-scheme for more information. *See also* **What is NIAP?**, below.

Q. What is a CCTL?

A. **CCTL** stands for Common Criteria Testing Lab. These testing labs are information technology (IT) computer security testing laboratories accredited to conduct IT security evaluations for conformance to the Common Criteria.

In the United States, the National Institute of Standards and Technology (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) accredits CCTLs to meet National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) requirements and conduct IT security evaluations for conformance to the Common Criteria.

A list of all CCTLs is located at www.commoncriteriaportal.org/public/developer/index.php?menu=9.

"Common Criteria Testing Lab" is the U.S. term; similar terms are used in other countries. *See* http://en.wikipedia.org/wiki/Common_Criteria_Testing_Laboratory for more information.

Q. What is Common Criteria/ISO-15408?

A. **Common Criteria/ISO-15408** is the standard for Common Criteria for Information Technology Security Evaluation, an international security certification standard for IT products. This Common Criteria standard describes a framework in which IT users specify security requirements for a product, and vendors implement products and make claims about their products' security. Authorized Common Criteria Testing Laboratories (CCTLs) evaluate the submitted products to determine if they actually meet the claims.

Formally, Common Criteria (CC) is "a common language and structure for expressing IT security requirements in a manner that allows those requirements to be used to evaluate allegedly conforming products."

There is an international CC Recognition Arrangement for EAL1–4 systems. There are currently 12 issuing countries: Australia, Canada, France, Germany, Japan, the Netherlands, New Zealand, Norway, the Republic of Korea, Spain, the UK, and the USA. These countries will also accept EAL1–4 certificates from 12 accepting countries: Austria, Czech Republic, Denmark, Finland, Greece, Hungary, India, Israel, Italy, Singapore, Sweden, and Turkey.

A current list of participating countries can be found at www.commoncriteriaportal.org/public/content/natscheme.html.

Currently, there is no CC recognition arrangement at EAL5–7. Without this agreement in place, each country must establish its own scheme for high-level (EAL5–7) evaluation. *See* **What is CCEVS?**, above.

Q. Is there a Common Criteria/ISO-15408 primer available?

A. Yes. The **Common Criteria Introduction** document is available at www.commoncriteriaportal.org/public/files/ccintroduction.pdf.

Q. Where can I get the latest copy of the Common Criteria?

The latest version of Common Criteria and the Common Evaluation Methodology documents is available at www.commoncriteriaportal.org/public/developer/index.php?menu=2.

Q. Which products have been evaluated by the Common Criteria?

A. The full list of all products evaluated by the Common Criteria standard is available at www.commoncriteriaportal.org/public/developer/index.php?menu=6.

Q. When was the Common Criteria published?

A. Version 1.0 of the Common Criteria was published for comment in January 1996. After two years of reviews and trials were incorporated, version 2.0 was published in May 1998. The official version of the Common Criteria and the Common Evaluation Methodology is v3.1. It consists of three parts:

1. Introduction and General Model
2. Security and Functional Requirements
3. Security Assurance Requirements

CC documents are available at www.commoncriteriaportal.org/public/consumer/index.php?menu=2.

Q. What is DCID 6/3?

A. **DCID 6/3** is a standard for Protecting Sensitive Compartmented Information Within Information Systems created by the Director of Central Intelligence. The DCID 6/3 document describes the following security issues:

1. Roles and Responsibilities
2. Levels of Concern and Protection Levels
3. Confidentiality System Security Features and Assurances
4. Systems Integrity Security Features and Assurances
5. System Availability Security Features and Assurances
6. Requirements for Interconnected Information Systems and Advanced Technology

7. Administrative Security Requirements
8. Risk Management, Certification, and Accreditation

This document is available at www.fas.org/irp/offdocs/DCID_6-3_20Manual.htm.

Q. What is Defense-in-Depth?

A. **Defense-in-Depth** is a strategy that integrates people, operations, and technology capabilities to establish information assurance (IA) protection across multiple layers and dimensions. Successive layers of defense will cause an adversary who penetrates or breaks down one barrier to promptly encounter another Defense-in-Depth barrier, and then another, until the attack ends. [NSA]

Q. What is DITSCAP?

A. **DITSCAP** stands for DoD Information Technology Security Certification and Accreditation Process. This process:

1. Helps ensure that information systems operate at an acceptable level of risk
2. Provides a system that meets customer needs while adhering to risk guidelines

Note that DITSCAP was replaced by DIACAP on July 6, 2006.

For more information on DITSCAP, *see* http://iase.disa.mil/ditscap/DitscapFrame.html.

For DITSCAP to DIACAP Transition Guidelines, *see* http://iase.disa.mil/ditscap/diacap-transition-encl6.pdf.

Q. What is DIACAP?

A. **DIACAP** stands for DoD Information Assurance Certification and Accreditation Process. This process:

1. Updates key elements of DITSCAP with a focus on Information Assurance
2. Replaced DITSCAP processes as of July 6, 2006
3. Now accepts NIAP CC certificates without additional review

For more information on DIACAP, *see* http://iase.disa.mil/ditscap/interim-ca-guidance.pdf.

For DITSCAP to DIACAP Transition Guidelines, *see* http://iase.disa.mil/ditscap/diacap-transition-encl6.pdf.

Q. What are Evaluation Assurance Levels (EALs)?

A. **Evaluation Assurance Levels (EALs)** define a scale for measuring the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs). The following table provides a summary of EAL levels:

EAL Level	Definition	Requirements Spec	Functional Spec	HLD	Covert Analysis
EAL1	Functionally tested	Informal	Informal	Informal	No
EAL2	Structurally tested	Informal	Informal	Informal	No
EAL3	Methodically tested and checked	Informal	Informal	Informal	No
EAL4	Methodically designed, tested, and reviewed	Informal	Informal	Informal	"Obvious vulnerabilities"
EAL5	Semiformally designed and tested	Formal	Semi-formal	Semi-formal	"Moderate attack potential"
EAL6	Semiformally verified, designed, and tested	Formal	Formal	Semi-formal	"Systematic"
EAL7	Formally verified, designed, and tested	Formal	Formal	Formal	"Systematic"

Q. What is a Foundational Threat?

A. A **Foundational Threat** is a threat that attacks the foundation of a secure application platform, rendering it ineffective from a security standpoint. Foundational threats include Bypasses, Compromises, Tamperings, Cascades, Covert Channels, Viruses, and Subversions.

Q. What is HAIPE?

A. **HAIPE** stands for High Assurance Internet Protocol Encryptor, an NSA crypto device. These devices are built by network vendors like Cisco, General Dynamics, Mitre, Harris, ViaSat, and other companies that use the HAIPE crypto system and APIs.

Q. What is Information Assurance (IA)?

A. **Information Assurance** is a strategy to insure that systems incorporate protection, detection, and availability, with the objective to reduce amount of security critical code and increase examination of security-critical code. [NSA]

IA is defined as the set of measures intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration

of information systems by incorporating protection, detection, and reaction capabilities. These measures are planned and executed by the Information Assurance Directorate (IAD) of the National Security Agency/Central Security Service (NSA/CSS). [NSA]

There are five IA pillars:

- Availability
- Integrity
- Authentication
- Confidentiality
- Nonrepudiation

These pillars and any measures taken to protect and defend information and information systems, and to provide for the restoration of information systems, constitute the essential underpinnings for ensuring trust and integrity in information systems.

Q. What is MILS?

A. **MILS** stands for Multiple Independent Levels of Security (or Safety or Separation). MILS is a layered software architecture (kernel, middleware, applications, and communications) for building "multilevel secure (MLS) systems" with high assurance that multiple separated entities (kernel, middleware, applications) will be able to operate and communicate exactly as dictated by specified safety and security policies, each at its own safety or security classification level as required, and all certified under Common Criteria to the appropriate Evaluation Assurance Level (EAL6 or higher for the OS).

MILS is a system that supports multiple, separated entities, each operating at a different classification level (safety/security/domains). MILS systems enforce:

1. Software architecture that supports MLS and MSLS
2. Robust time and space partitioning scheduler
3. Secure information flow, data isolation, periods processing, and damage limitation (safety/security/domains)

Q. What is MLS?

A. **MLS** stands for Multilevel Security. An MLS system securely processes data of differing classifications, such as guards, downgraders, firewalls, data fusion, and databases. Prior to MILS, in most cases, an MLS systems required redundant hardware for each classification of data.

Q. What is MSLS?

A. **MSLS** stands for Multi-Single-Level Security. An MSLS system securely separates data of differing classifications—such as communications platforms and infrastructures—one level at a time. Prior to MILS, in most cases, an MSLS required redundant hardware for each classification of data.

Q. What is NEAT?

A. **NEAT** stands for **N**on-Bypassable, **E**valuatable, **A**lways Invoked, and **T**amper-Proof. This term describes the fundamental characteristics of a separation kernel (SK).

Q. What is NIAP?

A. **NIAP** stands for National Information Assurance Partnership, a partnership of the National Security Agency and the National Institutes of Technology, and is the U.S. Government organization that administers the CCEVS in the U.S. *See* **What is CCEVS?**, above.

Q. What is NIAS?

A. In moving Information Assurance (IA) forward to protect the National Information Infrastructure (NII), a **National Information Assurance Strategy (NIAS)** was formed to encourage mutual cooperation and acceptance of common objectives. This strategy, built on the following five cornerstones, articulated the IA pillar concepts as a national framework that unified the U.S. Government's IA efforts:

1. Cyber-security awareness and education
2. Strong cryptography
3. Good security-enabled commercial information technology
4. An enabling global Security Management Infrastructure
5. A civil defense infrastructure equipped with an attack sensing and warning capability and coordinated response mechanisms

Q. What is NSTISSP 11?

A. **NSTISSP 11** stands for National Security Telecommunications and Information Systems Security Policy. This national policy governs the acquisition of Information Assurance (IA) and IA-enabled information technology products that protect national security information. This policy states that:

1. Effective July 1, 2002, all COTS IA and IA-Enabled products *must* be evaluated
2. Evaluation must be done by the NIAP Evaluation and Validation Program (CCEVS)
3. Evaluation will be conducted by an accredited commercial laboratory (a CCTL in the U.S.; *see* **What is a CCTL?**, above)
4. Evaluation must be done using an NSA or NSA-approved process

Waivers have been granted in the past, but Daniel Wolf, Director of IAD for the NSA, stated in 2003: "No more waivers." (quoted from DHS-OSD Software Assurance Workshop, October 3, 2005).

For more information, see http://niap.bahialab.com/cc-scheme/nstissp-faqs.cfm.

Q. What is PCS?

A. **PCS** stands for **Partitioning Communication System**. PCS*express* is a product from Objective Interface Systems (OSI) that enables trusted communication between partitions. More information is available at www.ois.com.

Q. What is a Protection Profile (PP)?

A. A **Protection Profile (PP)** is a standard set of security requirements for a category of products. Examples of Protection Profiles are the Separation Kernel Protection Profile (SKPP), File System Protection Profile (FSPP), and the MILS Network Stack Protection Profile (MNSPP).

A complete list of Protection Profiles is available at www.commoncriteriaportal.org/public/developer/index.php?menu=7.

Q. What is robustness?

A. The **robustness** of an evaluated product is the level of confidence in the protection provided to the security services it supports. [NIAP]

In addition, robustness is to the level of security functionality, level of assurance, and level of security application in a communications product. NIAP categorizes products into three groups: basic, medium, and high robustness. These are categories of environment for which a Target of Evaluation (TOE) can exist.

Q. What is a Security Policy Manager?

A. A **Security Policy Manager** controls data flow using Security Policies, typically in a MILS separation kernel.

Q. What is a Security Target (ST)?

A. A **Security Target (ST)** describes the security claims made for the Target of Evaluation (TOE) and how the TOE meets those requirements (often by claiming conformance to Protection Profiles (PPs). The TOE security threats, objectives, requirements, and summary specification of security functions and assurance measures together form the primary inputs to the ST.

Q. What is a Target of Evaluation (TOE)?

A. A **Target of Evaluation (TOE)** is the actual target (processor/hardware/BSP/operating system/applications) that will be evaluated in a security analysis.

Q. Where can I find additional security resources?

A. Additional **CCEVS resources** are available at www.nsa.gov/ia/industry/niap.cfm. Click on "CCEVS" for more information on Common Criteria.

Additional **NIAP resources** are available at www.nsa.gov/ia/industry/niap.cfm. Click on "NIAP" for more information.

A list of **NSA acronyms** is available at www.nsa.gov/ia/acronyms.cfm?MenuID=10.

Complete **Common Criteria** information is available at www.commoncriteriaportal.org.