

## Introducing the FAA Protection Profile Library

### The Beginning

The National Information Assurance Acquisition Policy, NSTISSP #11, was issued January 2000. This policy recommended (by January 2001), and then mandated (by July 2002) the use of Common Criteria evaluated products in national security systems. The phrase “national security systems” is interpreted to include critical infrastructure systems like those for which FAA is responsible, especially since the events of September 2001.

This web page has been created to facilitate the integration of the Protection Profiles into the FAA system engineering lifecycle and acquisition management system (AMS) process.

Five key goals drove this project:

- The Protection Profile library should be expanded to apply to all FAA systems, not just mission critical NAS systems, since FAA Order 1370.82 applies to all systems.
- Protection Profiles should grow beyond a “one size fits all” template and acknowledge differences in system size, complexity, risk, and technology.
- Security requirements should not be repeated in multiple places; rather they should be captured in one document and appropriate references made to it.
- Lifecycle documentation should be developed once with the goal of reusing it to satisfy multiple purposes: Common Criteria, security certification and authorization (C&A), FAA system engineering lifecycle documentation requirements, AMS, and other contractual requirements.
- Lifecycle documentation should be proportional to system risk and criticality.

To achieve these goals, several new features have been added to the Protection Profile library and several additional analytical processes have been completed.

### 18 Protection Profiles are now in the Library

The FAA Protection Profile library now contains 18 different Protection Profiles organized by:

- **System risk/criticality** -- high risk/critical system, moderate risk/essential system, or low risk/routine system
- **Technology and security enclave** -- WAN, LAN/Facility communications, or application system

- **System mission** -- Mission Critical (NAS) or Mission Support/Administrative

The system risk and criticality categories correspond to NAS-SR-1000 3.8.5 and FIPS PUB 199 definitions. Security functional requirements, security assurance requirements, security management requirements, and security audit requirements were all tailored based on system risk and criticality. Tailoring resulted in a lower number of requirements and less rigorous requirements for moderate and low risk systems. Furthermore, security requirements were allocated to security enclaves based on technology: WAN, LAN/Facility Communications, or Applications System. As expected, not all requirements apply to all three security enclaves. **[See the Protection Profile panel]**

### **Complete Requirements Traceability and Modularity**

Low-level security requirements in the Protection Profile were derived from the high-level information security requirements in NAS-SR-1000 3.8.5, providing complete requirements traceability. The ten high-level information security requirements in NAS-SR-1000 3.8.5 were used to construct 10 functional packages (or security subsystems):

- Level of security functionality and security integrity
- Security training
- Integrity
- Availability
- Access control
- Security audit
- Confidentiality
- Identification and authentication
- Recovery
- Security management

All high and low-level access control requirements are assigned to one functional package; confidentiality requirements are assigned to another functional package, and so forth. This modularity of requirements allows the FAA and the system developer to design, build, and test the 10 functional packages on independent timelines, if desired. **[See the Requirements Traceability Matrix panel]**

### **Mapping to FAA System Engineering Lifecycle Documentation Requirements**

Common Criteria artifacts, produced as a result of executing the security assurance requirements, are mapped to the documentation requirements of the FAA system engineering lifecycle. The artifacts produced by the Common Criteria methodology align directly with the FAA system engineering lifecycle documentation requirements; hence there is no duplication of effort. **The Common Criteria artifacts meet all the requirements of 20 of 24 (or 83%) of the documents normally required by the FAA system engineering lifecycle. The security assurance activities and artifacts also satisfy 19 of 29 (or 65.5%) of the subtasks required by the new security certification and authorization (C&A) standard NIST SP 800-37. [See CC Artifacts mapping panel]**

### **Language for Statement of Work (SOW) and DIDs are provided**

Language to incorporate in contractual documents, such as the Statement of Work (SOW), and Data Item Descriptions (DIDs) are provided. Specifically, standardized language is provided for SOW subsections 2 Applicable Documents, 4.1.1 Security Functional Requirements, 4.1.2 Security Assurance Requirements, and 5.1 Security Deliverables. In addition, DIDs are provided for 8 categories of lifecycle documentation which are required by the Common Criteria:

- Configuration management
- Delivery and operation
- System development
- User guidance
- Lifecycle support
- Testing
- Vulnerability assessment
- Maintenance of security assurance

The DIDs emphasize the technical content (not the format), which is derived from the content and presentation of evidence elements specified in the security assurance requirements. The DIDs are in final form and are ready to be incorporated into a Screening Information Request (SIR) or Request for Proposal (RFP) package. [See the SOW Inserts and DIDs panels]

### **The Protection Profiles are ready to use**

The Common Criteria element operations, component dependencies, hierarchies, security audit requirements, and security management requirements have all been completed in the Protection Profile library; no further action is required in this regard; the Protection Profiles are in final form.

### **Requirements Allocation and Tailoring**

Table A summarizes the allocation of low-level security requirements by security enclave and system risk and criticality. Table B illustrates the requirements decomposition and tailoring by system risk and criticality.

Table A. Low-level Requirements Allocation by Security Enclave and System Risk/Criticality

<b>Security Enclave</b>	<b>High Risk/ Critical System</b>	<b>Moderate Risk/ Essential System</b>	<b>Low Risk/ Routine System</b>
WAN	72	72	60
LAN/Facility Communications	75	75	60
Application System	75	75	66

Table B. Requirements Decomposition by System Risk and Criticality.

Functional Package/ NAS-SR-1000 Reference	High-level Reqts.	High Risk			Moderate Risk			Low Risk		
		Class	Family	Component	Class	Family	Component	Class	Family	Component
<b>I. Security Functional Requirements (SFRs)</b>										
Level of Security Functionality and Integrity 3.8.5.A <sup>1</sup>	1	-	-	-	-	-	-	-	-	-
Security Training 3.8.5.B <sup>2</sup>	1	-	-	-	-	-	-	-	-	-
Integrity 3.8.5.C	1	2	14	15	2	14	15	2	13	14
Availability 3.8.5.D	1	2	4	4	2	4	4	2	4	4
Access Control 3.8.5.E	1	2	7	9	2	7	9	2	7	8
Security Audit 3.8.5.F	1	2	7	12	2	7	12	2	7	12
Confidentiality 3.8.5.G	1	4	8	11	4	8	11	3	5	5
Identification and Authentication 3.8.5.H	1	3	10	16	3	10	16	1	6	10
Recovery 3.8.5.I	1	2	2	3	2	2	3	2	2	3
Security Management 3.8.5.J	1	2	11	16	2	11	16	2	12	16
<b>Total</b>	<b>10</b>	<b>19</b>	<b>63</b>	<b>86</b>	<b>19</b>	<b>63</b>	<b>86</b>	<b>16</b>	<b>57</b>	<b>72</b>
<b>II. Security Assurance Requirements (SARs)</b>										
Configuration Management (ACM)	-	1	3	3	1	2	2	1	1	1
Delivery and Operation (ADO)	-	1	2	2	1	2	2	1	2	2
System Development (ADV)	-	1	4	4	1	4	4	1	3	3
Guidance Documents (AGD)	-	1	2	2	1	2	2	1	2	2
Lifecycle Support (ALC)	-	1	2	2	1	1	1	0	0	0
Tests (ATE)	-	1	4	4	1	4	4	1	3	3
Vulnerability Assessment (AVA)	-	1	5	5	1	3	3	1	2	2
Maintenance of Assurance (AMA)	-	1	4	4	1	4	4	1	4	4
<b>Total</b>	<b>-</b>	<b>8</b>	<b>26</b>	<b>26</b>	<b>8</b>	<b>22</b>	<b>22</b>	<b>8</b>	<b>17</b>	<b>27</b>
<b>Evaluation Assurance Level</b>		<b>EAL 3+</b>			<b>EAL 3+</b>			<b>EAL 2+</b>		

<sup>1</sup> This statement is a high-level global requirement. All the SFRs and SARs specified in a PP contribute to its fulfillment.

<sup>2</sup> Training is an operational security, not an information security requirement. As such, training is not something that can be specified in an IT security requirements specification. The security assurance requirements ensure that the necessary documentation is developed to support the training.

### **Requirements are correct, consistent, and complete**

Lastly, Section 6, the Rationale, was added to the Protection Profiles in the library. The Rationale proves that the set of security functional requirements and security assurance requirements specified in Section 5 of the Protection Profile are a complete, correct, consistent, coherent, and cohesive whole. The Rationale demonstrates that a system that conforms to the Protection Profile will provide a set of IT security counter-measures that are effective within the specified operational environment. The security objectives rationale presents evidence to demonstrate that stated security objectives are traceable and suitable to cover all identified assumptions, threats, and security policies. The security requirements rationale presents evidence to demonstrate that the stated security requirements are traceable and suitable to satisfy all security objectives. Both rationales prove that as a whole the security objectives and security requirements are necessary, appropriate, and sufficient.

The cost, schedule, and technical benefits from generating a Protection Profile rationale and having the Protection Profiles certified are significant. [Several studies conducted during the last decade, inside and outside the U.S., concluded that ~85% of the failures or latent defects in IT systems were due to erroneous or missing requirements.](#) Taking the time to prove and certify that requirements are correct prior to design and implementation saves a lot of potentially wasted time and resources; it is much easier, less expensive, and faster to fix an erroneous requirement found during the requirements analysis phase than one found in an already built system.