



***Security Certification  
&  
Accreditation:  
DITSCAP vs. DCID 6/3***

**Steve Welke**

Manager, Security Accreditation

[www.TrustedCS.com](http://www.TrustedCS.com)

Trusted Computer Solutions, Inc.  
2350 Corporate Park Drive, Suite 500  
Herndon, VA 20171 USA  
+1.703.318.7134 (Phone)  
+1.703.318.5041 (Fax)

***White Paper***

# Security Certification and Accreditation: DITSCAP vs. DCID 6/3

Steve Welke  
Manager, Security Accreditation  
Trusted Computer Solutions, Inc.  
2350 Corporate Park Drive, Suite 500  
Herndon, VA 20171 USA  
+1.703.318.7134 (Phone)  
+1.703.318.5041 (Fax)

## 1. Introduction

The concept of security certification and accreditation (C&A) can be visualized as the “Good Housekeeping Seal of Approval” applied to automated information systems (AISs). The C&A process must assess whether the benefits of operating an AIS in a particular manner in a particular environment outweigh the accompanying risks. A highly-effective cleaning agent that burns its user’s skin unless steel gloves are worn is not likely to get the “Good Housekeeping Seal” for most environments; however, a slightly less-effective cleaning agent that poses no burn risks to uncovered skin is likely to receive approval. Similarly, a very sensitive, high-speed AIS that is wide open to attack via the Internet is not likely to be accredited; however, a slightly slower AIS that is not accessible via the Internet and is resistant to known network vulnerabilities is likely to be accredited. Certification and accreditation are formally defined as follows:

**Certification** – A comprehensive evaluation of the technical and nontechnical security features of an automated information system (AIS) and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and implementation meets a set of specified security requirements. [NST92]

**Accreditation** – A formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards. [NST92]

### 1.1. A Little History

The C&A process has been carried out in one form or another for many years. Although this author has not been able to find definitive history on its origins or evolution, it became clear by 1992 that C&A had been carried out long enough to result in enough different approaches to make it very difficult to compare results. The Office of Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) directed the Defense Wide Information Systems Security Program (DISSP) to create standardized requirements and processes for accreditation of computers, systems and networks in its August 19, 1992, memorandum, “The Defense Information Systems Security Program” [DIS92]. A security process improvement working group was formed to develop this standard process. Their task was to develop a standard C&A process

that would meet the policies defined in Department of Defense (DoD) Directive 5200.28 [DoD88], Public Law (PL) 100-235 [PL98], Office of Management and Budget (OMB) Circular A-130, Appendix III [OMB96], Director of Central Intelligence (DCID) 1/16 [DCI88] and DoD Directive 5220.22 [DoD80].

The DISSP, chaired by the Defense Information Systems Agency (DISA) and in coordination with the National Security Agency (NSA) and the Services and Agencies throughout the DoD, developed a standard C&A process to minimize the risks associated with non-standard security implementations across shared infrastructures and end systems. The DoD Information Technology Security Certification and Accreditation Process (DITSCAP), whose instruction was published in December 1997 (DoDI 5200.40 [DoD97]) and whose application manual was updated in July 2000 (DoD 8510.1-M [DoD00]), integrates security directly into the system lifecycle and is designed so that it can be applied uniformly across DoD. The primary C&A document in the DITSCAP is called the System Security Authorization Agreement (SSAA).

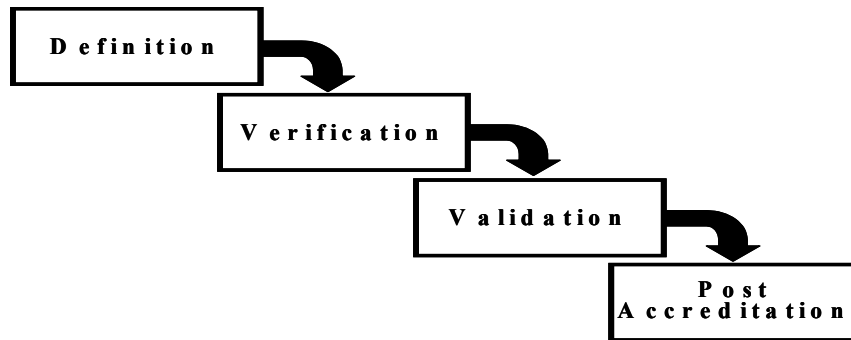
DCID 6/3 [DCI99], the directive published in June 1999 that replaces DCID 1/16, establishes the security policy and procedures for storing, processing, and communicating classified Intelligence information in AISs. While the DISSP working group took DCID 1/16 into consideration in creating the DITSCAP, the DCID 6/3 directive does not reference the DITSCAP. Instead, it may be based on DCID 1/16, and the primary C&A document in the DCID 6/3 directive is called the System Security Plan (SSP). The DCID 6/3 “application manual,” the *DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation Guide* that was updated in April 2001 (DIMD DS-2610-142-01 [DCI01]), does reference the DITSCAP and renames the primary C&A document to be an SSAA; confusion still reigns, however, as the DCID 6/3 SSAA is completely different from the DITSCAP SSAA.

## 1.2. Overview

This paper compares the DITSCAP and DCID 6/3 approaches to C&A. Section 2 describes the DITSCAP approach and Section 3 describes the DCID 6/3 approach. Section 4 compares the two approaches, identifies issues with documentation formats, and provides recommendations to resolve the issues. Section 5 provides conclusions.

## 2. DITSCAP

As shown in Figure 1, the DITSCAP approach consists of four phases. Phase 1 (*Definition*) is the longest phase. The objective of this phase is to agree on the intended system mission, environment, architecture, security requirements, certification schedule, level of effort, and resources required to achieve accreditation. The first phase culminates with a documented agreement (i.e., the first draft of the SSAA and most of its appendices) of the approach and the results of the above activities. Phase 2 (*Verification*) includes activities that verify compliance of the system with previously agreed upon security requirements (i.e., analysis of the system design and development of test plans). Phase 3 (*Validation*) includes activities that evaluate the fully-integrated system (i.e., execution of test plans and recording of test results) to validate system operation in a specified computing environment with an acceptable level of residual risk. The third phase culminates in an accreditation decision from the DAA, called an approval to operate (ATO). Phase 4 (*Post Accreditation*) includes activities that monitor system management and operation to ensure that an acceptable level of residual risk is preserved.



**Figure 1. DITSCAP Phases.**

As shown in Appendix A, the C&A documentation created during the four DITSCAP phases consists of a main body “executive summary” (the SSAA) and 18 associated appendices. Per guidance from the Secret and Below Interoperability (SABI) office [SABI01], the SSAA must adhere strictly to the format provided, and the appendices must be numbered exactly as shown with no additional appendices allowed. Unfortunately, this required list does not include several appendices that the author considers essential based on experience:

- A stand-alone C&A plan,
- A system security architecture document,
- A procedural site security management plan (sometimes called a Trusted Facility Manual),
- A technical administrator’s guide (sometimes called a Trusted Facility Manual),
- A technical user’s guide (sometimes called a Security Features User’s Guide), and
- A roadmap system security test plan.

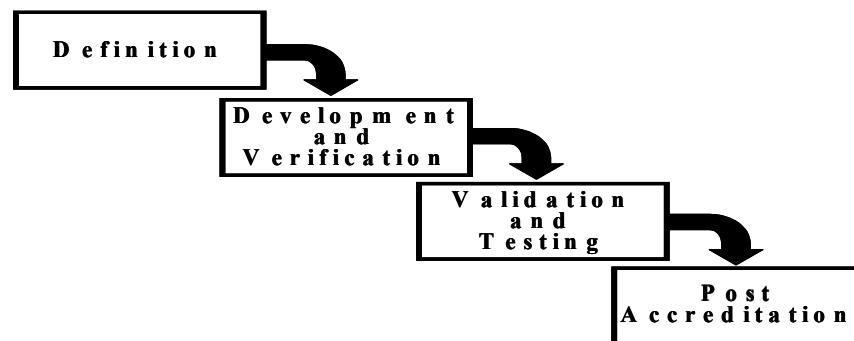
Before discussing what to do with these “missing” appendices, it is worth a quick sidebar to address the overloaded term “Trusted Facility Manual (TFM).” The Trusted Computer System Evaluation Criteria (TCSEC) [DoD85], also known as the “Orange Book,” defines a TFM as a technical administrator’s guide. The TCSEC “Rainbow Series” guideline on Trusted Facility Management [NCSC89] introduces confusion by using a similar term with the same acronym to describe procedural security management; a TFM (as defined in the TCSEC) is part of “trusted facility management.” The confusion became complete when “TFM” started being used as the title of procedural security management plans. So, one must be clear when discussing a TFM.

With no direction provided in any of the DITSCAP documents (i.e., the instruction [DoD97], the document guidelines [DoD98], or the application manual [DoD00]), the author pursued additional guidance from the SABI office on how to handle the missing appendices. The SABI guidance was to reference the administrator’s and user’s guides in Appendix J, System Rules of Behavior, and to [awkwardly] place the other four essential appendices as “sub-appendices” under Appendix I, System Documentation or Applicable Development Artifacts.

### **3. DCID 6/3**

As shown in Figure 2, the DCID 6/3 approach consists of four phases. Phase 1 (*Definition*) is the longest phase. The objective of this phase is to agree on the intended system mission, security requirements, C&A boundary, schedule, level of effort, and resources required for the

certification effort. The first phase concludes when all responsible organizations adopt the SSAA and concur that its objectives have been met (i.e., as documented in the first draft of the SSAA and most of its appendices). Phase 2 (*Development and Verification*) focuses on the system development activity and ensuring that the system complies with the previously agreed upon security requirements and constraints (i.e., analysis of the system design and development of test plans). Phase 3 (*Validation and Testing*) produces the required evidence (i.e., execution of test plans and recording of test results) to demonstrate that the system has an acceptable level of residual security risk. The third phase culminates with the DAA using this evidence to make an informed decision to grant approval to operate the system. Phase 4 (*Post Accreditation*) includes several activities to ensure that an acceptable level of residual security risk is preserved.



**Figure 2. DCID 6/3 Phases.**

As shown in Appendix B, the C&A documentation created during the four DCID 6/3 phases consists of a main body “executive summary” (the SSAA), five associated appendices, and six associated attachments. Per guidance from the Office of Naval Intelligence (ONI) [ONI01], the SSAA and appendices must adhere strictly to the format provided; additional sections and appendices are allowed, however, as long as they do not interfere with the exact numbering provided in the DoDIIS templates [DCI01]. Unfortunately, this required list does not include several appendices that the author considers essential based on experience:

- A concept of operations (CONOPS),
- A stand-alone C&A plan,
- A system security architecture document,
- A technical administrator’s guide (sometimes called a Trusted Facility Manual), and
- A technical user’s guide (sometimes called a Security Features User’s Guide).

Since additional appendices are allowed, it is no problem to include these missing appendices at the end of the DCID 6/3 C&A documentation set.

#### **4. Comparing the Two Approaches**

Comparison of the DITCAP and DCID 6/3 approaches will be broken down into two parts: the processes, and the documentation sets.

#### **4.1. The Processes Are Essentially the Same**

The DoDIIS guide [DCI01] claims that the DCID 6/3 “C&A process has been harmonized with the DITSCAP;” comparison demonstrates that this claim is true. Both approaches have four phases with almost identical names, and the activities within each DCID 6/3 phase have almost all of the same names as the activities identified in the DITSCAP phases. The level of detail and the exact implementation of the activities differs between the two instructions, but the intent is the same. There are some differences based on context (e.g., DITSCAP’s SABI vs. DCID 6/3’s TSABI, DITSCAP’s four C&A levels vs. DCID 6/3’s five Protection Levels), and there is an occasional “extra” activity (e.g., “Preparation” in DITSCAP Phase 1, “Configuration Management” in DCID 6/3 Phase 3). Overall, however, someone familiar with one of these C&A processes should have no difficulty understanding the activities in the other C&A process.

#### **4.2. The Contents in the Documentation Sets Are Similar – the Formats Are Not**

The DoDIIS guide states that “the security documentation used to support the DoDIIS system security certification process is modeled after the SSAA used to support certification under the DITSCAP.” Comparison demonstrates that this statement is false. It should have said that the DoDIIS-Tailored SSAA is modeled after the System Security Plan (SSP) described in DCID 6/3 because there is a very strong resemblance between these two formats; the DCID 6/3 SSAA format demonstrates little resemblance to the DITSCAP SSAA format. More fully, the formats of the entire DCID 6/3 C&A documentation set (i.e., the SSAA and its associated appendices/ attachments) demonstrate little resemblance to the DITSCAP C&A documentation set formats.

That said, the content of the documentation sets is ultimately not that different. It is not surprising that the content is similar, because the C&A evidence that a DAA needs is not mysterious or complicated – C&A evidence is very similar to sound software engineering evidence:

- Identify why the system is needed in the first place,
- Develop a policy to meet that need,
- Identify system requirements that meet the policy,
- Design a system that meets the requirements,
- Build a system that meets the design,
- Develop test plans that demonstrate the system meets its requirements,
- Execute the tests, and
- Assess the test results from a risk management perspective.

The remainder of this section identifies issues with the way the different formats arrive at similar content, along with the author’s recommendations for resolution.

##### **4.2.1. The Audience and Purpose Are Unclear**

Neither approach clearly identifies the audience and purpose for the various documents that are required.

**Recommendation:** Clarify the audience and purpose for each document so that a set of useful, value-added references results from conducting and completing the C&A process. Table 1 suggests the audience and purpose for each document.

**Table 1: Audience and Purpose for Each C&A Document.**

<b>Document</b>	<b>Audience</b>	<b>Purpose</b>
<b>SSAA</b>	DAA	Executive summary of key information in the appendices.
<b>C&amp;A Plan</b>	DAA, CA, PM, User Representative	Primarily boilerplate, but it identifies the key players (its audience), lays out the typical C&A activities/deliverables/responsibilities, and contains the C&A schedule.
<b>CONOPS</b>	All	The first document written, it is a high-level document that identifies the mission need and operational requirements; it describes the existing system, identifies its shortcomings, and presents the proposed concept to overcome those shortcomings.
<b>Security Policy</b>	DAA, CA, PM	Based on the CONOPS, high-level INFOSEC properties (typically found in government regulations) plus site-specific INFOSEC needs.
<b>Security Requirements</b>	CA, Testers, PM, Developers	Based on the Security Policy, specific “what” statements (typically found in standards like the Common Criteria) that drive the system design/architecture.
<b>Architecture</b>	Developers, Testers	Based on the CONOPS and the Security Requirements, “how” design information that leads to system implementation.
<b>Test Plans &amp; Procedures (e.g., CT&amp;E, ST&amp;E)</b>	CA, Testers	Based on the Security Requirements and the Architecture, specific tests that verify how the system and its environment meet their security objectives.
<b>Requirements Traceability Matrix</b>	CA, Testers	A mapping between the Security Requirements and the Test Procedures to ensure testing is necessary and complete.
<b>Test Results &amp; Residual Risk Assessment</b>	CA, PM, Developers	Based on implementation of the Test Procedures, these two documents capture the residual risk of operating the system in its particular environment.
<b>Site Security Management Plan</b>	ISSM	Based on the CONOPS, the Security Policy, and the Security Requirements, site-specific procedural information for implementing a secure environment.
<b>Administrator’s Guide</b>	ISSO	Based on the Architecture, technology-specific instructions for installing, configuring, and maintaining the system and its security capabilities.
<b>MOUs &amp; C&amp;A Letters</b>	DAA, CA, PM	Official statements from the DAA(s) and CA.

#### 4.2.2. Lots of Redundant Information

Both approaches put the same information in multiple documents, which leads to inconsistencies between different sections on the same topic, makes it difficult to know where to look for all the details on a particular topic, and makes maintenance a big challenge.

**Recommendation:** Have one detailed description of each pertinent topic in the appropriate document (based on the document's audience and purpose), and then reference that detail as needed in other documents.

#### 4.2.3. Where is the C&A Documentation Savings?

When the DITSCAP was developed, it claimed to greatly reduce the amount of documentation. In fact, this claim is misleading. It still takes time and pages to create the C&A evidence that a DAA needs (see Section 4.2); the DITSCAP simply moved much of that evidence to appendices, and then focused on the SSAA itself that is, in fact, much shorter. The real change with the DITSCAP is that documentation now can be found in standard places with standard names. (Yes, we can argue whether the standard formats and terms are the best – which I do! The concept of standardization, however, is a beneficial one.)

**Recommendation:** Concede that C&A evidence takes time and pages no matter how you split it up – the real savings is in reuse and comprehension over multiple C&A efforts through standard formats and terms.

#### 4.2.4. What is the “SSAA”?

Most people think the SSAA is the entire set of C&A documentation. Technically, this understanding is correct as long as it is clear that the appendices are part of the SSAA. Practically, however, the term “SSAA” is used to describe the main body without its appendices. There is often confusion about how much detail should be in the main body vs. the appendices. Using the practical definition, DITSCAP has a short SSAA and a lot of appendices; DCID 6/3 has few appendices and a much bigger SSAA.

**Recommendation:** Use the practical definition of “SSAA” to describe the chapters in the main body (as I have done throughout this paper). The SSAA should be viewed as an “executive summary” of the information in the appendices – it summarizes important details for the DAA, and will not be reused outside of the C&A process. The details belong in the appendices that will be reused by appropriate personnel outside of the C&A process. The DCID 6/3 SSAA is much too detailed and is very redundant with the DCID 6/3 TFM – the DITSCAP SSAA format should be adopted.

#### 4.2.5. What/Where is the “TFM”?

As discussed in the sidebar in Section 2, the term “TFM” can be confusing. DCID 6/3 uses the term to describe a site security management plan, and DITSCAP uses the term to describe a technical administrator's guide. DCID 6/3 has put all of its site security management information into one document – DITSCAP has most of that information spread out over a number of documents (i.e., Appendices K, L, M, and O).

**Recommendation:** Avoid the term “TFM” altogether – use the terms “Site Security Management Plan” and “Administrator’s Guide” to clarify each document’s content. Always require a Site Security Management Plan, even if it contains pointers to other documents.

#### **4.2.6. What is the Overall Approach to Testing?**

DCID 6/3 has a single test plan (Certification Test Procedures). DITSCAP has two test plans to distinguish technology-specific tests (CT&E Plan) from site-specific procedural tests (ST&E Plan). The DITSCAP approach saves time because the technical CT&E tests can be executed once exhaustively in a laboratory environment (and then spot-checked at each site), and the non-technical ST&E tests can be executed at each site in the form of an interview. Neither approach provides a means to describe other types of testing (e.g., developmental, operational).

**Recommendation:** Add a System Security Test Plan appendix that provides a roadmap for all types of testing that are performed. Use the DITSCAP approach of splitting up the technology-specific tests and the site-specific procedural tests to save test time. Add clarity by changing the titles to Technical Test Plan (instead of CT&E) and Non-Technical Test Plan (instead of ST&E).

#### **4.2.7. Missing Appendices**

DCID 6/3 is missing a CONOPS, and both sets are missing a stand-alone C&A plan and a system security architecture document.

**Recommendation:** Add these missing appendices.

#### **4.2.8. Where is the DCID 6/3 Security Policy?**

DCID 6/3 claims that it “establishes the security policy and procedures for storing, processing, and communicating classified intelligence information in information systems (ISs).” There is a “Policy” portion of DCID 6/3, but there are also “policy” statements in the “Manual” portion of the directive. Since the purpose of a policy is to drive the requirements and the DCID 6/3 requirements are already identified in the directive, it may not be essential to clearly identify the entire security policy. It would be nice, however, to have a place to document site-specific policy additions; a separate Security Policy would provide that place and would have the added benefit of clarifying the scope of the DCID 6/3 policy.

**Recommendation:** Add a Security Policy as a DCID 6/3 appendix to provide a place to document site-specific policy additions and to clarify the scope of the DCID 6/3 policy.

## **5. Conclusions**

DITSCAP and DCID 6/3 have the same intent – to ease the burden and increase the understanding of C&A by standardizing activities that should be performed and deliverables that should be produced. There are some minor contextual differences between the activities in the two approaches, but someone familiar with one of these C&A processes should have no difficulty understanding the activities in the other C&A process. The DCID 6/3 C&A documentation formats demonstrate little resemblance to the DITSCAP C&A documentation formats. The content of the documentation sets, however, is ultimately not that different. By implementing the recommendations presented in Section 4.2, the best of both documentation formats could be leveraged to create a single “format” that would promote the common intent of both approaches.

## References

- [DCI88] Director of Central Intelligence Directive (DCID) 1/16, *Security Policy on Intelligence Information in Automated Systems and Networks*, March 14, 1988.
- [DCI99] DCID 6/3 (replaces DCID 1/16), *Protecting Sensitive Compartmented Information Within Information Systems*, June 5, 1999.
- [DCI00] Defense Intelligence Management Document [unnumbered], *DoD Intelligence Information Systems (DoDIIS) Certification and Accreditation Guide*, April 2000.
- [DCI01] Defense Intelligence Management Document DS-2610-142-01, *DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation Guide*, April 2001.
- [DIS92] Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) Memorandum, *The Defense Information Systems Security Program (DISSP)*, August 19, 1992.
- [DoD80] DoD Directive 5220.22, *Industrial Security Program*, December 8, 1980.
- [DoD85] DoD 5200.28-STD, *Trusted Computer System Evaluation Criteria*, December 1985.
- [DoD88] DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988
- [DoD97] DoD Instruction 5200.40, *DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)*, December 30, 1997.
- [DoD98] DITSCAP Guidelines, *DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP) [Guidance CD-ROM]*, Version 1.0, June 1998.
- [DoD00] DoD 8510.1-M, *DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP) Application Manual*, July 31, 2000.
- [NST92] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, *National Information Systems Security (INFOSEC) Glossary*, June 1992.
- [ONI01] Office of Naval Intelligence (ONI) Feedback, *Discussions with Brian Walter in relaying his understanding of ONI guidance*, August 2001 – October 2001.
- [PL98] Public Law 100-235, *Computer Security Act of 1987*, January 8, 1998.
- [NCSC89] NCSC-TG-015, *A Guide to Understanding Trusted Facility Management*, Version 1, October 18, 1989.
- [OMB96] Office of Management and Budget Circular No. A-130, *Management of Federal Information Resources*, February 8, 1996.
- [SABI01] Secret and Below Interoperability (SABI) Office Feedback, *Discussions with Joe Jevcak in relaying his understanding of SABI guidance*, June 1999 – October 2001.

## Appendix A. DITSCAP Required Format

This appendix contains the required format for the DITSCAP SSAA and its appendices [DoD00].

1. MISSION DESCRIPTION AND SYSTEM IDENTIFICATION
  - 1.1 System Name and Identification
  - 1.2 System Description
  - 1.3 Functional Description
    - 1.3.1 System Capabilities
    - 1.3.2 System Criticality
    - 1.3.3 Classification and Sensitivity of Data Processed
    - 1.3.4 System User Description and Clearance Levels
    - 1.3.5 Life Cycle of the System
  - 1.4 System CONOPS Summary
2. ENVIRONMENT DESCRIPTION
  - 2.1 Operating Environment
    - 2.1.1 Facility Description
    - 2.1.2 Physical Security
    - 2.1.3 Administrative Issues
    - 2.1.4 Personnel
    - 2.1.5 Communications Security (COMSEC)
    - 2.1.6 TEMPEST
    - 2.1.7 Maintenance Procedures
    - 2.1.8 Training Plans
  - 2.2 Software Development and Maintenance Environment
  - 2.3 Threat Description
3. SYSTEM ARCHITECTURAL DESCRIPTION
  - 3.1 SYSTEM ARCHITECTURE DESCRIPTION
  - 3.2 System Interfaces and External Connections
  - 3.3 Data Flow
  - 3.4 Accreditation Boundary
4. SYSTEM SECURITY REQUIREMENTS
  - 4.1 National and DoD Security Requirements
  - 4.2 Governing Security Requirements
  - 4.3 Data Security Requirements
  - 4.4 Security Concept of Operations
  - 4.5 Network Connection Rules
  - 4.6 Configuration Management
  - 4.7 Reaccreditation Requirements
5. ORGANIZATIONS AND RESOURCES
  - 5.1 Organizations
  - 5.2 Resources
  - 5.3 Training
  - 5.4 Other Supporting Organizations
6. DITSCAP PLAN
  - 6.1 Tailoring Factors
    - 6.1.1 Programmatic Considerations
    - 6.1.2 Security Environment
    - 6.1.3 IS Characteristics
    - 6.1.4 Reuse of Previously Approved Solutions
  - 6.2 Tasks and Milestones
  - 6.3 Schedule Summary
  - 6.4 Level of Effort
  - 6.5 Roles and Responsibilities

- Appendix A. Acronyms
- Appendix B. Definitions
- Appendix C. References
- Appendix D. Concept of Operations (CONOPS)
- Appendix E. Information System Security Policy (ISSP)
- Appendix F. Security Requirements Document (SRD) and/or Requirements Traceability Matrix
- Appendix G. Certification Test & Evaluation (CT&E) Plan And Procedures
- Appendix H. Security Test & Evaluation (ST&E) Plan and Procedures
- Appendix I. System Documentation or Applicable Development Artifacts
- Appendix J. System Rules of Behavior
- Appendix K. Incident Response Plan
- Appendix L. Contingency Plan
- Appendix M. Personnel Controls and Technical Security Controls
- Appendix N. Memorandums of Agreement
- Appendix O. Security Education, Training, and Awareness (SETA) Plan
- Appendix P. Test and Evaluation Results
- Appendix Q. Residual Risk Assessment (RRA) Results
- Appendix R. Certification and Accreditation (C&A) Statements

## Appendix B. DCID 6/3 Required Format

This appendix contains the required format for the DCID 6/3 SSAA, its appendices, and its attachments [DCI01].<sup>1</sup>

1. SYSTEM GENERAL INFORMATION
  - 1.1 SECURITY ADMINISTRATION
    - 1.1.1 System Identification
    - 1.1.2 Points of Contact
  - 1.2 MISSION
    - 1.2.1 Purpose and Scope
    - 1.2.2 OED Usage
2. SECURE FACILITY DESCRIPTION
  - 2.1 FACILITY LAYOUT
  - 2.2 SYSTEM LAYOUT
  - 2.3 PHYSICAL ENVIRONMENT
  - 2.4 TEMPEST
3. DESCRIPTION OF THE SYSTEM
  - 3.1 SYSTEM ARCHITECTURE AND OPERATIONS
  - 3.2 SYSTEM LAYOUT AND DATA FLOW DIAGRAMS
  - 3.3 CLEARANCE LEVEL/NEED-TO-KNOW REQUIREMENTS
  - 3.4 FOREIGN NATIONAL ACCESS
  - 3.5 CLASSIFICATION OF DATA PROCESSED
    - 3.5.1 Classification and Compartments
    - 3.5.2 Dissemination Controls
  - 3.6 DCID 6/3 LEVELS OF CONCERN
    - 3.6.1 Confidentiality
    - 3.6.2 Integrity
    - 3.6.3 Availability

---

1. There is another "DoDIIS guide" [DCI00] provided on an official ONI CD-ROM that adopted an SSAA format almost identical to the DITSCAP format described in Appendix A. This DITSCAP-like SSAA format was apparently rejected as inferior between April 2000 and April 2001.

- 3.7 DCID 6/3 PROTECTION LEVELS
- 3.8 NON-U.S. CITIZEN ACCESS
- 3.9 INTERCONNECTION INTERFACE DESCRIPTION
  - 3.9.1 Direct Network Connections
  - 3.9.2 Procedures for Identifying and Documenting System Connectivity
  - 3.9.3 External System Connections
  - 3.9.4 Procedures for External System Connections
  - 3.9.5 External Connections to Lower Classifications or to Foreign Nationals
  - 3.9.6 Data Flow Diagrams for External Connections
  - 3.9.7 Communications Protection for External Connections
  - 3.9.8 Networking
  - 3.9.9 Indirect Connections (i.e., "sneaker-net")
- 3.10 SYSTEM DESIGN DOCUMENTATION
- 4. HARDWARE
  - 4.1 HARDWARE IDENTIFICATION
  - 4.2 CUSTOM-BUILT HARDWARE
- 5. SOFTWARE
  - 5.1 SOFTWARE IDENTIFICATION
  - 5.2 SECURITY CONFIGURATION GUIDES
  - 5.3 SERVICES AND PROTOCOLS
  - 5.4 ELECTRONIC MAIL
- 6. DATA STORAGE
  - 6.1 STORAGE MEDIA AND CONTROL
  - 6.2 MEDIA HANDLING AND SECURITY
  - 6.3 ARCHIVE/RESTORE PROCEDURES
  - 6.4 ARCHIVE PROTECTION
  - 6.5 DISASTER RECOVERY
- 7. SECURITY REQUIREMENTS
  - 7.1 THREATS AND VULNERABILITIES
  - 7.2 USER ACCESS AND OPERATION
    - 7.2.1 Access Controls
    - 7.2.2 Account Management
    - 7.2.3 Authenticator Management
    - 7.2.4 Passwords Assigned to System Users
    - 7.2.5 Passwords Assigned to Privileged Users
    - 7.2.6 Changing Passwords
    - 7.2.7 Generating Passwords
    - 7.2.8 Failed Login Controls
    - 7.2.9 Reinstating Locked Accounts
  - 7.3 USER GROUPS AND CONTROLS
    - 7.3.1 User Groups
    - 7.3.2 System Files
    - 7.3.3 System Access Rights
    - 7.3.4 Audit Log Access
    - 7.3.5 Privileged Users
    - 7.3.6 Guides and/or Manuals for Privileged Users
    - 7.3.7 Technical Control for User Access
    - 7.3.8 Discretionary Access Control (DAC)
    - 7.3.9 Need-to-Know Assurance
    - 7.3.10 Mandatory Access Control (MAC)
    - 7.3.11 DAC Plus Implementation
  - 7.4 SECURITY SUPPORT STRUCTURE PROTECTION
    - 7.4.1 Component Protection
    - 7.4.2 Login Authentication Protection

- 7.4.3 Security Support Structure Validation Procedures
- 7.5 SECURITY FEATURES AND ASSURANCES
  - 7.5.1 Incident Reporting
  - 7.5.2 Remote Access
  - 7.5.3 Configuration Management
  - 7.5.4 Security Integrity Validation
  - 7.5.5 Other Security Features
  - 7.5.6 Recovery Procedures
  - 7.5.7 After Hours Processing
  - 7.5.8 System Start-up
  - 7.5.9 Compliance Monitoring
  - 7.5.10 Non-Repudiation
  - 7.5.11 Transaction Rollback
- 7.6 AUDITING
  - 7.6.1 Audit Procedures
  - 7.6.2 Notification Banner
  - 7.6.3 Unique Identification and Association
  - 7.6.4 Audit Trail Protection
  - 7.6.5 Audited Information
  - 7.6.6 Audited Activities
  - 7.6.7 Audit Review Responsibility
  - 7.6.8 Audit Discrepancies
  - 7.6.9 Testing the Security Posture of the System
- 7.7 CLASSIFICATION MARKINGS AND LABELS
  - 7.7.1 Hardware Labeling
  - 7.7.2 Storage Media Labeling
  - 7.7.3 Printout Labeling and Control
  - 7.7.4 Electronic Marking
  - 7.7.5 Media/Hardware not Marked
- 7.8 MAINTENANCE PROCEDURES
  - 7.8.1 Maintenance/Repair Procedures
  - 7.8.2 Procedures for Lower Cleared or Maintenance Personnel
  - 7.8.3 System Hardware Maintenance Logs
  - 7.8.4 Software Used for Maintenance
  - 7.8.5 Remote Diagnostics
- 7.9 SANITIZATION AND DESTRUCTION
  - 7.9.1 Hardware Sanitization
  - 7.9.2 Storage Media Sanitization
- 7.10 SOFTWARE SECURITY PROCEDURES
  - 7.10.1 Software Procurement and Introduction
  - 7.10.2 Evaluating Software for Security Impacts
  - 7.10.3 Virus and Malicious Code Protection
  - 7.10.4 Software/Data Integrity Protection
- 7.11 MEDIA MOVEMENT
  - 7.11.1 Storage Media Transfer
  - 7.11.2 Data Transfer Accountability
- 7.12 HARDWARE CONTROL
  - 7.12.1 Hardware Transfers
  - 7.12.2 Hardware Relocation
  - 7.12.3 Hardware Release
  - 7.12.4 Hardware Operation and Maintenance
  - 7.12.5 Hardware Introduction
- 7.13 WEB PROTOCOL AND DISTRIBUTED/COLLABORATIVE COMPUTING
  - 7.13.1 Web Services Control

- 7.13.2 Mobile Code
- 7.13.3 Collaborative Computing
- 7.13.4 Distributed Processing
- 7.14 WIRELESS DEVICES
- 7.15 PUBLIC KEY INFRASTRUCTURE
- 8. SECURITY AWARENESS PROGRAM
  - 8.1 PROGRAM DESCRIPTION
  - 8.2 PROGRAM DOCUMENTS
- 9. INTERCONNECTION SECURITY AGREEMENT (ISA)
- 10. MEMORANDUM OF AGREEMENT (MOA)
- 11. AVAILABILITY
  - 11.1 RESTORING THE SYSTEM
  - 11.2 BACKUP COMMUNICATIONS CAPABILITY
  - 11.3 POWER BACK-UP SYSTEM
  - 11.4 PREVENTION OF DENIAL OF SERVICE ATTACKS
  - 11.5 PRIORITY PROTECTION
- 12. EXCEPTIONS
- 13. GLOSSARY

- Appendix A. Security Requirements Traceability Matrix (SRTM)
- Appendix B. Certification Test Procedures (Required for PL2 and above)
- Appendix C. Certification Test Report
- Appendix D. Certification/Approval to Operate/Accreditation Documents
- Appendix E. Trusted Facility Manual
- Attachment 1 Facility Layout
- Attachment 2 System Layout
- Attachment 3 Hardware List
- Attachment 4 Software List
- Attachment 5 Interface Security Agreements (ISAs)
- Attachment 6 Memorandums of Agreement (MOAs)