

Navigating the SABI/CDS Process

September 2005



Navigating the Secret and Below Interoperability (SABI) / Cross Domain Solutions (CDS) Process

This paper is an update to [WEL03] that captures the following changes:

- Change of program name from Secret and Below Interoperability (SABI) to Cross Domain Solutions (CDS). For clarity, both names (SABI and CDS) are retained in this paper because “cross domain solution” is a generic term used for multiple purposes.
- Change in documentation approach from the full System Security Authorization Agreement (SSAA) plus appendices to a Cross Domain Appendix (CDA).
- Addition of a pre-qualification process that involves the Cross Domain Solutions Assessment Panel (CDSAP) and the Community Jury.

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. DITSCAP Origins

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 (ASD/C3I) 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” [ASD92]. 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], 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).

1.2. SABI/CDS Origins

The ASD/C3I directed NSA and DISA to create the Secret and Below Interoperability (SABI) program in its March 20, 1997, memorandum, "Secret and Below Interoperability" [ASD97]. In September 2003, SABI changed its name to Cross Domain Solutions (CDS). For clarity, both names (SABI and CDS) are retained in this paper because "cross domain solution" is a generic term used for multiple purposes.¹

SABI/CDS's mission is "to ensure, within acceptable risk, the integrity of the Defense Information Infrastructure (DII)" [SABI00]. Part of SABI/CDS's mission is to implement a community-based C&A process for systems that connect a Defense Information System Network (DISN) asset (e.g., the SIPRNet) to a network at a lower classification (e.g., the NIPRNet or the Internet). In carrying out their mission, SABI/CDS has mandated that the DITSCAP approach to C&A must be used. SABI/CDS has, however, tailored the DITSCAP documentation requirements and added additional activities that are carried out by various SABI/CDS organizations.

1.3. Why this Paper?

This paper describes the various organizations that are involved in the SABI/CDS C&A process and how to navigate, in coordination with the DITSCAP approach, through the activities that are required by these organizations. Section 2 provides a brief overview of the DITSCAP approach and how TCS supports the roles involved. Section 3 describes the various SABI/CDS organizations and presents lessons that TCS has learned in supporting customers to address the requirements of each organization. Section 4 provides conclusions.

1. See Footnote 3.

2. DITSCAP Approach

The DITSCAP approach consists of activities, documentation, and roles. This section provides an overview of the activities and documentation, and then describes how TCS supports customers in working with the roles to execute the required activities and produce the required documentation.

2.1. DITSCAP Activities

As shown in Figure 1, the DITSCAP activities are grouped into four phases:²

- Phase 1, Pre-Certification (*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, Certification (*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, Accreditation (*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 – an approval to operate (ATO).
- Phase 4, Post-Accreditation (*Post-Accreditation*), includes activities that monitor system management and operation to ensure that an acceptable level of residual risk is preserved.

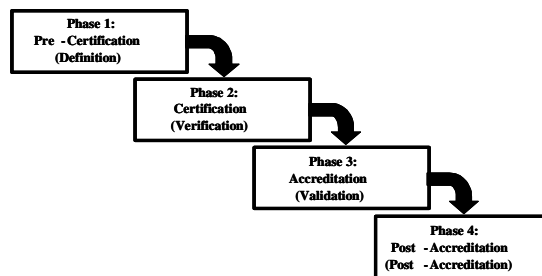


Figure 1. DITSCAP Phases.

2.2. DITSCAP Documentation

C&A documentation should add value, not simply be thrown together to satisfy the C&A process and then become shelfware when the process is complete. To that end, TCS has streamlined the set of DITSCAP documents [WEL00] and developed an approach to making each DITSCAP

2. Each phase in Figure 1 has two names, one being in parentheses. TCS has found the names used by the National Computer Security Center [NCSC96] to be much more descriptive and useful for customers. Thus, this paper presents both the NCSC and the DITSCAP names (with the DITSCAP names in parentheses).

document a value-added asset [WEL02]. In particular, TCS puts all of the required content into an appropriate DITSCAP appendix and views the SSAA as an executive summary of the content in the appendices. Table 1 summarizes the audience and purpose for each DITSCAP document.

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

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

2.3. DITSCAP Roles

The DITSCAP approach requires four key roles (the same person can fill multiple roles):

- The *Designated Approving Authority (DAA)* accredits the system prior to its operation. The DAA is the official with the authority to formally assume responsibility for operating an AIS or network at an acceptable level of risk [DoD97].
- The *Certification Authority (CA)* works for the DAA to formally certify the system. The CA is responsible for making a technical judgment of the system's compliance with requirements, identifying and assessing the risks associated with operating the system, coordinating certification activities, and consolidating the final C&A package [DoD97].
- The *Program Manager (PM)* ensures that security measures are implemented to adequately satisfy the security specification and that any residual risks are identified. The PM is the person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of the system [DoD97].
- The *User Representative (User Rep)* provides the user voice in identifying the users' roles, responsibilities, and capabilities. The User Rep is the individual or organization that represents the user or user community in the definition of system requirements [DoD97].

TCS recommends identifying three more roles to effectively complete the DITSCAP approach:

- The *Information System Security Officer (ISSO)* assists in the development of the system security policy and ensures compliance on a day-to-day basis. The ISSO reports security incidents, provides user training, and identifies changes that may require reaccreditation.
- The *Developer* implements the information system, manages the development environment, delivers the final product, and trains user personnel.
- The *C&A Facilitator* coordinates all of the C&A activities and produces C&A documentation to successfully complete the C&A process.

Figure 2 illustrates how the four key roles required by the DITSCAP work together with the three additional roles (with TCS serving as the C&A Facilitator).

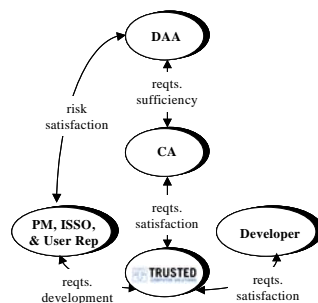


Figure 2. TCS Coordination of DITSCAP Roles.

Throughout the DITSCAP process, TCS (the C&A Facilitator) works primarily with one person at the customer site who coordinates gathering information and setting up meetings with the appropriate roles. During Phase 1, the PM, ISSO, and User Rep provide information about the mission (CONOPS), verify the security policy (ISSP) and security requirements (SRTM), start documenting site security procedures (SSMP), and identify and schedule C&A tasks (C&A Plan). The DAA and CA should review and agree to all of these Phase 1 documents. During Phase 2, the CA reviews the Developer's design (Architecture), implementation (Admin and User Guides)

and test plan/procedures (CT&E and ST&E) in preparation for executing technical and non-technical tests. During Phase 3, the CA executes tests, documents test results (Test Report), assesses the residual risk (RRA), and presents a recommendation (CA Letter) to the DAA. The DAA then makes an accreditation decision (DAA Letter). During Phase 4, the DAA and ISSO periodically review and analyze the security of the system to confirm that it continues to be managed and operated securely.

The DITSCAP provides a standard set of activities, documents, and roles for a local site to use in assessing the site's risk of operating a system. If the site is following good system engineering practices, a properly implemented DITSCAP approach should only require a small amount of additional effort to demonstrate the residual risk to the DAA. If the site is not following good system engineering practices, a properly implemented DITSCAP approach should point out the deficiencies and will require a more significant amount of additional effort to demonstrate the residual risk to the DAA. SABI/CDS attempts to leverage the work invested in the DITSCAP approach for the DISN community to use in assessing the community's risk of operating a system.

3. SABI/CDS Approach³

The SABI/CDS C&A process follows the basic principles in the DITSCAP approach, but requires 10 additional activities among seven additional organizations using a customized documentation approach to gain approval for a system that connects a DISN asset to a network at a lower classification. This section provides an overview of the SABI/CDS documentation, organizations, and activities, and presents lessons learned in going through the SABI/CDS process many times.

3.1. SABI/CDS Documentation

The SABI/CDS process presupposes the existence of a full set of DITSCAP documentation for the high-side network that connects to a DISN asset. The cross domain solution then becomes one more node added to the high-side network. Thus, SABI/CDS requires the creation of a Cross Domain Appendix (CDA), which addresses the particulars of the new node and is added as another appendix to the existing high-side network's SSAA.

TCS has learned that the CDA itself is not sufficient. The CDA also points to several other DITSCAP-like documents that are specific to the new cross domain solution. Table 2 summarizes the audience and purpose for the CDA and the DITSCAP-like documents to which it points.

3. There is a Top Secret and Below Interoperability (TABI) process that uses the same approach as SABI/CDS. There is also a Top Secret SCI and Below Interoperability (TSABI) process that uses a very different approach (different organizations, different documentation). All three processes assess "cross domain solutions" for use in their communities.

Table 2: Audience and Purpose for Each SABI/CDS C&A Document.

Document	Audience	Purpose
CDA	DAA, CA, SSES, CDTAB, DSAWG	Identifies mission need and operational requirements
CDS Security Requirements Traceability Matrix	CA, Testers, PM, Developers, SSES, CDTAB	Specific “what” statements that drive the CDS design/architecture. Eventually maps Requirements to Test Procedures so testing is necessary and complete.
CDS Architecture	Developers, Testers, SSES	“How” design that leads to CDS implementation.
CDS Test Plans & Procedures (e.g., CT&E, ST&E)	CA, Testers, SSES, CDTAB	Based on the Security Requirements and the Architecture, specific tests that verify how the CDS and its environment meet their security objectives.
CDS Test Results & Residual Risk Assessment	CA, PM, Developers, SSES, CDTAB	Based on implementation of the Test Procedures, these two documents capture the residual risk of operating the CDS in its particular environment.
CDS Administrator’s & User’s Guides	ISSO, SSES	Based on the Architecture, technology-specific instructions for installing, configuring, maintaining and using the CDS and its security capabilities.

3.2. SABI/CDS Organizations

The *SIPRNet Connection Approval Office (SCAO)* is the administrative arm of the SABI/CDS process. The *Cross Domain Solutions Assessment Panel (CDSAP)* is the initial technical review board for the SABI/CDS pre-qualification process. The *Community Jury* is the initial management review board for the SABI/CDS pre-qualification process. The *System Security Engineering Support (SSES)* team is a technical team that reviews the customer’s DITSCAP documentation. The *National Security Agency (NSA)* testing team performs NSA Certification Test and Evaluation (CT&E) on cross domain solutions. The *Cross Domain Technical Advisory Board (CDTAB)* is the final technical review board for the SABI/CDS process. The *DISN Security Accreditation Working Group (DSAWG)* is the final management review board for the SABI/CDS process.

3.3. SABI/CDS Activities

As described in Figure 3, there are 10 steps to completing the SABI/CDS process:

1. The customer (usually the PM) requests an account on the SABI/CDS SIPRNet web site and receives a “Request #”. The customer has 45 days from this point to: (a) submit initial CDA information to the SCAO, (b) have a G2 representative validate the need for the proposed solution, and (c) have the Service Combatant Agency prioritize the proposed solution.

2. The SCAO submits information to the CDSAP in priority order.
3. The CDSAP determines whether a better alternative is available, and whether the proposed solution should go through NSA testing. The CDSAP submits its findings to a Community Jury.
4. The Community Jury verifies the CDSAP findings and instructs the SCAO to issue a "SABI/CDS Ticket #".
5. The SCAO assigns the SABI/CDS Ticket to a specific SSES team.
6. TCS begins facilitating interactions between the customer and the SSES team.
7. NSA performs technical testing on the guarding solution, and provides findings to the SSES team and the CDTAB.
- 8 & 10. Once TCS has updated the customer's CDA documentation with SABI/CDS-required information, the DAA has signed off on accepting the residual risk, the SSES team has reviewed the updated documentation and completed a risk assessment, NSA has performed technical (CT&E) testing, and the SCAO has received an updated SIPRNet Connection Approval Process (SIPRCAP) package from the customer, the SSES team provides a recommendation to the CDTAB. *[Before and after on-site (ST&E) testing is performed]*
- 9 & 11. Once the SSES team's recommendation has been briefed to the CDTAB, the CDTAB provides a recommendation to the DSAWG. *[Before and after on-site (ST&E) testing is performed]*
12. Once the CDTAB's recommendation has been briefed to the DSAWG, the DSAWG provides the SCAO with a recommendation to approve this connection to a DISN asset (e.g., the SIPRNet).

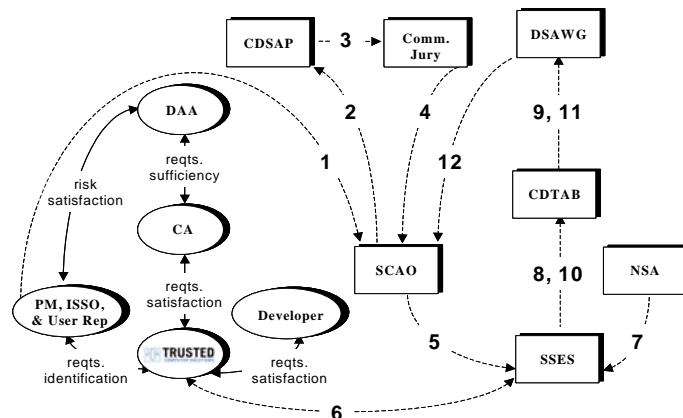


Figure 3. TCS Coordination of SABI/CDS Organizations.

3.4. SABI Lessons Learned

The following lessons have been learned:

1. Going through the SABI/CDS C&A process does not allow a site to bypass performing its own C&A effort. Rather, the SABI/CDS process presumes that a local, DITSCAP-based site process is being performed. The SABI/CDS process requires its 10 steps to be performed in addition (in parallel, hopefully) to the site's process.
2. *Both* site (DAA) and SABI/CDS (DSAWG) approval are required for a system to connect a DISN asset to a network at a lower classification. Sites will often think that either kind of

- approval is sufficient. The fact is that the CDTAB and DSAWG will not consider a system for approval until the DAA has signed off on accepting the residual risk, and the site must wait for DSAWG approval to officially connect and operate the system at their site.
3. The SABI/CDS process is the “long pole in the tent.” In addition to requiring 10 more steps, the execution of those SABI/CDS steps is constantly evolving based on technology and politics. SABI/CDS also requires some additional information to be included (e.g., Joint Vulnerability Assessment Program (JVAP) data). Thus, the SABI/CDS process must be engaged as early as possible.
 4. Having “NSA look at” the system is a SABI/CDS requirement. One NSA group supports the SABI/CDS process, and a separate NSA group (or groups) “looks at” or tests guarding solutions. NSA currently uses the term “CT&E” for their testing of a guarding solution. It is unclear whether NSA’s CT&E completely substitutes for the DITSCAP-required CT&E, but NSA testing is clearly required to participate in the SABI/CDS process. TCS is continually supporting products through NSA’s CT&E process, as political priority and NSA resources allow.
 5. The site must update its SIPRCAP package to include the new guarding solution in order to go before the CDTAB. The SIPRCAP package consists of a series of questions that the site must answer. The most important part of the SIPRCAP package is a network diagram showing the new guarding solution and where it will exist in the network topology.
 6. Having a SABI/CDS Ticket issued does not mean the site has approval to connect and operate the system at their site. The site has “SABI/CDS approval” only after the DSAWG’s recommendation to connect has been accepted.

4. Conclusions

The SABI/CDS process mandates use of the DITSCAP approach, but involves a separate set of interactions to gain approval for a system that connects a DISN asset to a network at a lower classification. This paper identifies the connection between the SABI/CDS process and the DITSCAP approach, and describes how to navigate through the activities required by the SABI/CDS process. It also presents lessons that TCS has learned while supporting numerous customers; these lessons must be understood to successfully complete the SABI/CDS process.

References

- [ASD92] 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.
- [ASD97] Office of Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)) Memorandum, *Secret and Below Interoperability*, March 20, 1997.
- [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.
- [NCSC89] NCSC-TG-015, *A Guide to Understanding Trusted Facility Management*, Version 1, October 18, 1989.
- [NCSC96] NCSC-TG-031, *Certification and Accreditation Process Handbook for Certifiers*, Version 1, July 1996.
- [NST92] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, *National Information Systems Security (INFOSEC) Glossary*, June 1992.
- [OMB96] Office of Management and Budget Circular No. A-130, *Management of Federal Information Resources*, February 8, 1996.
- [PL98] Public Law 100-235, *Computer Security Act of 1987*, January 8, 1998.
- [SABI00] SABI Guidelines, *Secret and Below Interoperability (SABI) [Guidance CD-ROM]*, Version 1.0, June 2000.
- [SABI01] Secret and Below Interoperability (SABI) Office Feedback, *Discussions with Joe Jevcak in relaying his understanding of SABI guidance*, June 1999 – October 2001.
- [WEL00] Welke, Steve, *Streamlining DITSCAP Documentation*, TCS White Paper, January 2000.
- [WEL02] Welke, Steve, *Security C&A: DITSCAP vs. DCID 6/3*, TCS White Paper, January 2002.
- [WEL03] Welke, Steve, *Navigating the SABI Process*, TCS White Paper, July 2003.