THE DEPARTMENT OF DEFENSE INFORMATION ASSURANCE SUPPORT ENVIRONMENT[1]

Jack Eller
DISA, IPMO
701 South Courthouse Rd.
Arlington, VA 22204-4507

Barry Stauffer
CORBETT Technologies, Inc.
701 South Courthouse Rd.
Arlington, VA 22204-4507

Logicon, Inc.
P. O. Box 6340
Annapolis, MD 21401

228 N. Saint Asaph St.
Alexandria, VA 22314-2517

Abstract

The Department of Defense (DoD) Information Assurance Support Environment (IASE) has been developed to support Information Assurance (IA) staff and to implement uniform Information System Security (INFOSEC) Certification and Accreditation (C&A) practices throughout the DoD. IA staff and C&A practitioners (Help Clients) across DoD will be able to contact their parent Service or Agency Support Center for assistance. These Support Centers will be linked to share information. Self Help features will provide the Client with access to IA support information, descriptions of uniform C&A practices and procedures, notices and technical discussions, formats and examples of documentation, and access to responses to previous IA questions. Search engines and browsers will expedite Client retrieval of desired information. For assisted help, the Client will also be able to contact IA Support Providers, leveraged by a robust Help Desk system. Trouble ticketing, information servers, and tiered access to specialists and experts will offer Clients a full spectrum of help in resolving their IA and C&A questions.

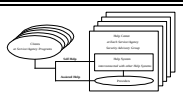
Key Words

Accreditation, Certification, Defense Information Infrastructure (DII), Department of Defense (DoD), DoD Information Technology Security Certification and Accreditation Process (DITSCAP), Designated Approving Authority (DAA), Help Desk, Information Assurance, Information Technology, Information Systems Security (INFOSEC), Support Environment.

1. Introduction

The Department of Defense (DoD) Information Assurance Support Environment (IASE) has been developed to support Information Assurance (IA) staff and to implement uniform Information System Security (INFOSEC) Certification and Accreditation (C&A) practices throughout the DoD. The IASE, Figure 1, establishes both technical and administrative mechanisms to provide consistent detailed IA and C&A guidance across DoD. It will support personnel directly involved with IA, certification, accreditation, acquisition, system development, maintenance, operation, or administration, whether they are performing, managing, or endorsing the C&A actions. These individuals who are seeking help are referred to as support clients

[1] The Information Assurance Help Environment has been developed for DISA IPMO under Logicon, Inc. Contract DAAB07-91-D-B519



(Clients), and those who are advising them, or providing help, are referred to as support providers (Providers). Clients across DoD will be able to contact their parent Service or Agency Support Center for assistance. The Service and Agency Support Centers will be linked to share information throughout the Support Environment. The Client will receive assistance in the form of both Self Help and Assisted Help through state-of-the-art technology.

The Self Help features will provide the Client access to the Service or Agency Support Center with descriptions of C&A practices and procedures, access to notices and technical discussions related to C&A, formats and examples of documentation, and access to the responses to previous questions. Self Help will expand the capabilities normally available through access to Web sites with hyper-text documentation.

Assisted Help will expand upon the capabilities provided by Help Desk systems. The Client will be able to contact C&A experts through access to the support system. Upon contacting the Providers (Support Center staff leveraged by the support system), the Client will ask the Provider C&A questions related to the Clients specific system or situation. The Provider will access a database of trouble tickets containing previous questions. If the current request is similar to an existing trouble ticket, the Provider will first review the response to the trouble ticket and, if appropriate, provide that information to the Client. If the request does not match an existing trouble ticket, a new trouble ticket will be opened and remain open until the request is fully satisfied. This new response will now be available to future searches.

2. Support Environment Concept

Automated help in a variety of forms is commonplace in today's world. It is used in the introduction and support for almost every new product. Today those clients seeking support are encouraged to initially use the self help features, e.g., hyper-text web pages like FAQs (frequently asked questions), bulletin boards, list servers, and chat groups. If the required information is not available or found, the client is encouraged to contact a Support Center for assisted help. The Support Center staff (Providers) are often leveraged with technology such as trouble ticket systems for tracking open issues or questions and accessing closed issues. Such

Figure 2. Help Environment Client Options.

technology can leverage DoD Service and Agency security advisory staffs in supporting DoD systems and programs staff with IA guidance and assistance.

The C&A portion of the Support Environment will be based upon the information provided in the DITSCAP and other related C&A information issued by the National Computer Security Center [4, 5]. The DITSCAP was developed as the common process to be uniformly implemented across all of DoD. The DITSCAP integrates security directly into the system life cycle with a focus on the security of the infrastructure to meet the needs defined by the Defense Information Systems Security Program study and the security process improvement working group.

The support Providers will be coordinated through Support Centers, each technically leveraged by a support system. Support Centers are planned for DoD Services or Agencies to help clients within that organization. Clients will be encouraged to make full use of the Self Help and to use the Assisted Help whenever necessary. Both the Providers and Clients will access the support system, although not equally. All of the Support Centers will be interconnected to realize a shared and distributed IASE across DoD. The Clients, Providers, and Centers with the support systems form the C&A Support Environment, Figure 1.

2.1 Support Centers

The Support Center, Figure 2, will provide clients support through both Self Help and Assisted Help options.

Self Help. The Support Client will have ready access to a wide range of IA and C&A information through Self Help features. The Self Help options will provide access to:

- General information regarding C&A process in terms of its phases, activities, and tasks.
- A notification system with IA and C&A notices from the DoD Service/Agency C&A experts.
- A repository of both C&A formats and examples for key artifacts, e.g., documentation, produced by C&A actions.
- An on-line discussion with peers regarding C&A-related topics.

- A repository of specific advice items previously provided by support providers.

The Self Help options will be directly accessible by on-line or isolated users. The items available will be searchable by key words, topical hierarchies, or system classifications, as appropriate. This information will be contained in the Self Help knowledge base.

Assisted Help. If the Client cannot find the information needed, or requires specific advice, the Client can obtain personal assistance from a Provider through the Assisted Help option. Support Providers will access the information and previously completed specific advice queries available through the Self Help. If the Client is seeking specific advice which is a new query, the Provider will provide an immediate answer or seek advice from other providers or experts. Open queries will be prioritized, re-prioritized periodically, and tracked until answered. To effectively support clients, the Providers at each DoD Service or Agency will be structured into three tiers based on expertise, namely C&A Assistants (Tier 1), C&A Specialists (Tier 2), and C&A Experts (Tier 3), Figure 3. Client's calls, whether by e-mail or phone, will first be fielded by the Tier 1 providers. If the Tier 1 provider is not able to respond to the query, it is escalated to Tier 2 providers, and then likewise escalated to Tier 3 providers, if necessary. This ensures prompt qualified attention to each call and effective use of limited experts. It should be noted that C&A queries requiring judgment decisions would not be considered by the Providers and should be referred to the staff of the Designated Approving Authority (DAA). The Assisted Help options will be accessible by on-line or isolated users.

2.2 Support System

Leveraging each DoD Service or Agency Support Center is a standard support system. The envisioned features and architecture of the support system are described below and shown in

Figure 4. This system will be used by IA and C&A Clients, and Providers, but not equally. Providers will have additional features available to them. In addition, there will be administrative features also available to system administrators. A suggestion or comment feature will be available to all users.

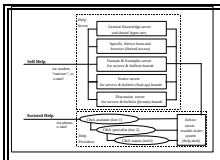


Figure 4. Support System Logical Architecture.

Self Help will be available to Service and Agency clients across the Internet or an Intranet such as NIPRNET or SPIRNET, whichever is deemed appropriate. For those isolated from such networks, a limited CD-ROM version could be made available and updated periodically. Pointers to the support systems can be provided on appropriate DoD Service/Agency home pages. Assisted Help will be available over appropriate networks by e-mail or by telephone. Furthermore, the Support Centers at the Services and Agencies and the Defense Information Systems Agency INFOSEC Program Management Office (IPMO) will be interconnected to create the technical side of a virtual Support Environment which supports all of DoD.

General Knowledge. The General Knowledge option will provide C&A information that describes the C&A process (DITSCAP) in terms of its process structure hierarchy - phases, activities, and tasks. It may include for phase, activity, or task the following:

- Description
- Components
- Milestone relationships
- Output contributions
- Other info sources
- Estimating costs
- Goals
- Sequencing
- Input descriptions
- Output formats
- Resource needs
- Start criteria
- Responsibilities
- Scheduling
- Output descriptions
- Output examples
- Resource qualifications
- Finish criteria

General knowledge is that core of information that describes the C&A process (DITSCAP), procedures, techniques, and tools. This is information which could be obtained by experience, detailed briefings, classes, or technical reading and would be applicable to any, or at least many systems. Managers, or management support staff may enter this area to obtain process overview information or access to INFOSEC related DoD directives, instructions or notices. Engineers may, however, seek very detailed information related to the process, activities, and tasks.

This information will be in a hyper-text form accessible and searchable by a standard web-browser. Clients may search this information by key words or role perspectives using the browser to review stored web pages. Information will be stored in a simple form and recoverable by the browser to ensure consistency and allow flexibility. Links will be established so that clients can traverse the information in logical, appropriate ways, e.g., within a task by role responsibilities or across a phase by descriptions.

Notices. The Notices options will provide notifications on key C&A topics. In this case each area will be populated with some initial notices to encourage Clients to visit topic areas. As the environment matures, clients may request new notice topics be added. The initial system may include notices on the following:

- C&A planning
- Security T&E planning
- Documentation
- C&A support tools
- Security T&E procedures
- Security Plans
- Security requirements
- H/W & S/W security issues
- Rules of Behavior

It is envisioned that this information will be posted on bulletin boards and list servers by the C&A experts. Clients may search this information by key words. Additionally, clients may subscribe to list servers or be subscribed based on role, function, or life-cycle perspective, as appropriate.

Discussions. The Discussions option will provide an opportunity for clients to carry-on discussions with other C&A practitioners, both in real-time and non-real-time. It is also anticipated the support system administrators or Service and Agency INFOSEC experts would use this capability as a medium to provide information to the field engineers performing certification and accreditation tasks. As the environment matures, clients may request new discussion topics be added. Initial discussion topics may include:

- DITSCAP phases
- DITSCAP activities
- DITSCAP tasks
- DITSCAP steps
- Requirements definition
- Security test & evaluation
- Life-cycle C&A issues
- Risk management
- Documentation
- C&A planning
- C&A support tools
- Responsibilities

These discussions will be hosted with chat groups for real-time discussions and forum bulletin boards or list servers for non-real time discussions. Clients will be able to join the discussions in which they are interested or want to participate. Live discussions can be held at scheduled times guided by a C&A expert or on ad hoc basis among interested peers.

Formats and Examples. The Formats and Examples option will provide access to a repository of formats, examples, worked samples of C&A documentation, past cases of C&A documentation, and C&A related or supporting information. The related or supporting information may include such items as:

• DoD & Federal Security Policy	• Automated tools	• Documentation support
• Security Plans	• Trusted Facility Manual	• Rules of Behavior
• IT System Security Management Procedures	• Security Awareness and Training Plans	• Risk Management Plans or Approaches
• Incident Response Plans	• Contingency Plans	• Incident Response Plans

This information will be in a simple library database management system accessible through a web-browser. Clients may search this information by key words.

Specific Advice. The Specific Advice Option will provide details on specific questions previously answered by C&A Support Providers. These answers will focus items about C&A process tasks and steps. Some of these specific knowledge items will be delineated according to life-cycle, function, or role perspectives, as well as indexed by the system classification scheme described in Enclosure 7 of the DITSCAP [1].

This information will be held in an advice server with a repository of completed responses available to clients in a read-only form. Clients may search this information by key words using a browser to access the advice server.

Advice Server. Support Providers will use an Advice Server to support them in fielding and responding to queries seeking specific advice as well as the repository of past responses. This server will be the workbench for the providers responding to specific advice calls, directly to the client as well as coordinating a difficult query among other support providers. It should support establishing a client query, tracking open queries, escalating, coordinating queries, and archiving a final response. Initially, the server would be "primed" with a number of predetermined responses.
A trouble ticket system will be used to provide such functionality and support to the Support Providers. The information in the trouble ticket system will be indexed by DITSCAP process item and be searchable by key words as well as time open, query priority, etc.

Tracking and Metrics. The support system will provide the ability to compile and deliver reports, metrics, and statistics needed to manage the support system. The metrics and statistics will provide the ability to identify priorities and greatest need through monitoring of the usage and subjects of greatest interest.

Suggestions and Complaints. The support system will provide the ability to collect and process client and provider suggestions and complaints. It is envisioned that a simple trouble ticket database will be created for this function, taking input through e-mail or by phone.

2.3 Support Providers

Provider support will be structured with a three tiered approach as depicted in Figure 3. The Tier 1 Provider (C&A Assistant) is the initial and central client point of contact. All assisted help queries enter here. Tier 1 handles basic problems and uses knowledge-based tools to resolve as many problems on the first call as possible. If the Tier 1 Provider cannot resolve the problem, it is escalated to Tier 2 (C&A Specialist) who handles the more advanced problems and provides

the support necessary to research and resolve the hard-to-find answers. Final escalation is to the Tier 3 Providers (C&A Experts) who are the technical experts and gurus with the expertise to resolve the most difficult problems. Note that a higher Tier will only field queries referred to them from a lower one.

The Tier 1 support staff should be trained in the DITSCAP and in the use of the automated Support System. Tier 2 staff should have some practical C&A experience, be trained in DITSCAP, and in the use of the automated Support System. Tier 3 staff should have extensive practical C&A experience, be trained in DITSCAP, and in the use of the automated Help System. They will also have access to DISA IPMO or DoD Service and Agency security technical staff for consultation as necessary.

The Providers will also develop and post notices across the Support Environment. Some of these may be advice to a specific query, which merits posting. The Providers may also monitor and contribute to discussions occurring in the Support Environment as well as advice provided to specific queries as part of an overall quality assurance program. Such a quality program could be accomplished on a priority basis using the tracking system to order items for review.

3. Users of the Support Environment

The Clients IASE are expected to span every role and function related to IA and INFOSEC C&A within DoD. Clients may vary from senior management and experienced technical professionals to entry level technical staff or military staff with their first introduction to INFOSEC C&A. The Clients experience is expected to range from seasoned professionals to those with little or no experience. Similarly the roles of the Clients are expected to be equally diverse. The Clients could have extensive experience within their role or be acting in that role for the first time. As government downsizes, contractor personnel may be performing in almost all certification and accreditation actions except for those endorsing actions by the DAA or Certifier.

The IASE will explicitly recognize clients based on their current perspectives to their C&A actions. It will delineate life-cycle perspectives (development, operation, maintenance), function perspectives (acquisition, use, accreditation, certification, engineering/administration), and role perspectives (manage, perform, endorse (authority role taking responsibility)). The DoD Inst 5200.28, Enclosure 8 [1], contains a detailed description of the various C&A roles and an overview of their responsibilities.

The Providers of the IASE will span levels of expertise commensurate with the three tiered structure. Moreover, they will be stationed at various DoD C&A Support Centers.

4. Summary of Advantages

The advantages of the IASE will be to realize the goal of more uniform C&A practice throughout the DoD through the promotion of standard practices. These results will be achieved by use of the current best practices. As a result, scarce resources now used to develop manuals may be directed toward the development of much needed C&A support tools. C&A standardization will be achieved near term, not at some future time.

The IASE provides the key to leverage the DoD resources. Service and Agency IA support groups will be enabled to empower their field staff performing C&A. Information will be shared not only from expert to novice but from peer to peer. The IASE provides the capability to place example documents, or document outlines and approved C&A documentation in a repository for all to use. For example, the definition of the security requirements for a new system can be greatly eased by the use of the security requirements prepared for a similar system. Likewise, through reuse, the preparation of detailed test procedures, a lengthy task, can be greatly reduced in both time and scope. As the documents are reused, improved versions can be placed in the repository for new Clients. The DITSCAP established the concept of system classes to promote this leveraging of information. In a very similar way the experts advice is leveraged by the IASE through the use of Self Help features and the trouble ticket concept.

There will also be a leverage through technology. As new techniques evolve, they can be rapidly provided to field C&A practitioners through the IASE assets. The experts will now be freed to monitor the process to provide direction and address difficult or common technical issues. When they provide support, that information will be immediately available to everyone within DoD. As new technology becomes available it can be rapidly introduced to everyone.

Key advantages with the IASE, include:

- Providing IA awareness and education, detailed C&A guidance, and C&A support through one environment by Self Help or Assisted Help.
- Capturing and providing best practices and understandings of C&A, where the C&A knowledge-base is an actual experience base and grows with use.
- Leveraging and empowering current resources as either support providers or support clients.
- Using technology as leverage in ways that commercial customer service environments do today and for which COTS products are available.
- Achieving uniform, consistent C&A across DoD by default, not by decree or chance.

References:

[1] DoD Instruction 5200.28, “Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP)”, Draft May 1997.
[2] Office of Management and Budget (OMB) Appendix III to OMB Circular No. A-130 - Security of Federal Automated Information Resources, February 1996.
[3] National Computer Security Center (NCSC) Certification and Accreditation Process Handbook for Certifiers (NCSC-TG-031), TBD.
[4] Introduction to Certification and Accreditation (NCSC-TG-029), January 1994
[5] National Computer Security Center (NCSC) Accreditor’s Guide (NCSC-TG-032), TBD