

Life Cycle Security and DITSCAP

by Mr. John Kimbell and Ms. Marjorie Walrath

For a successful technology, reality must take precedence over public relations, for nature cannot be fooled.

—Richard P. Feynman

With the announcement that the Department of Defense (DoD) will be spending \$1.5 billion on information systems security, many organizations, both public and private, have presented themselves as experts in network security in order to take advantage of this windfall. But posturing does not guarantee professional results and, in reality, many of those claiming to be security engineers and certifiers/accreditors have little in-depth experience in the field. In some cases, organizations are not familiar with DoD or federal department-specific regulations. They cannot relate to the manner in which the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) should be applied. Only an informed community can separate the nascent from the experts.

The Good, The Bad, and The Ugly

The relationship between security certification/accreditation and the information network system is a life cycle commitment; therefore, it is appropriate to be wary of an organization or business with a miraculous “one price, guaranteed delivery by a certain date” sales pitch. Some organizations approach security in the same manner as their other business

practices, relying heavily on marketing techniques to overcome their shortcoming. It is important to remember that although it is the foremost goal of a business to make money, the paramount goal of Government is to spend money for the general welfare of its citizens.¹ We in DoD have a well-defined responsibility to the American people, and must remember that if we make a mistake, we can damage the security posture of the entire nation.

Certification—Not Always Understood

Frequently, the C&A process is misunderstood. Many, if not most, people think that once their system has been certified they have a guarantee that it is operating in a totally secure mode. That is not what certification is all about. Consider the United States Department of Agriculture (USDA). Most of us are familiar with the phrase “Certified USDA prime,” or similarly, “Certified USDA Choice.” The USDA has seven different “Applicable Quality Grades” for beef.² The highest of these is “Prime” and the lowest is “Canner.” When a shipment of beef arrives for quality grading, it is certified as to its quality, processing, size, packaging, and delivery. Each shipment is graded against these requirements.

Therefore, even though all shipments are certified, there are varying degrees of quality. The same idea holds true for the security certification for information systems.

Certification in the context of information systems security means that the system has been analyzed as to how well it meets all of the security requirements that have been levied against it from various sources [AR380-19, the Orange book,³ specific system standard operating procedures (SOPs), etc.] So the final certification statement is really saying, “We have compared your system to all of these requirements (just like the USDA) and here is what we have found— your system meets 82% of these requirements. Of the 18% of the requirements that your system does not meet, X% are vulnerabilities that lead to extremely high risk, Y% are vulnerabilities that lead to high risk...” and so on.

Promises, Promises, Promises...

The DITSCAP is flexibly designed to accommodate the changes that are an integral part of the security certification and accreditation process. Many inexperienced companies drop the ball here. Their claim to provide a total systems C&A in a specified time is not achievable. First, if they are going to be involved in the certification process they must be involved in all four phases of that process, and there is simply no

way to determine how long each phase will last. Additionally, at the completion of each phase and before the next phase begins there is a chance for each of the proponents to negotiate or re-negotiate what they will do, and a chance to renegotiate cost. As the process unfolds there will quite often be changes to the system, and the DITSCAP's flexibility allows for these changes. However, many of the organizations claiming to be C&A experts choose to ignore the fact that these changes will occur in the development of any new system. They ignore the realities of changing requirements, thus inviting slipped timelines and additional costs. It is not enough to "certify the box"—they must be willing to look behind the box, around the box, and to see where the box leads. C&A is an iterative and evolutionary process.

Phase 1: Definition

The main proponents of the C&A process come together for the first time in phase one. These proponents are the designated approving authority (DAA), user representative, project manager (PM), and certifier. The DAA is the individual responsible for ensuring that the system operates with an acceptable level of risk. The certifier is the individual responsible for ensuring that the DAA has been given sufficient information regarding those risks.

It is in this initial phase that the DAA appoints the certifier by issuing an actual appointment letter listing that individual as certifier for the specific system being certified. For the remainder of the process the certifier will—

- Act as a trusted agent of the DAA
- Provide support to the DAA by conducting a comprehensive evaluation of both the technical and non-technical security features of the system under evaluation.
- Recommend to the DAA whether or not to accredit the system after the certification process is completed.

The DITSCAP also allows for the creation of certification teams under the direction of the certifier to support the certifier in the actual security testing.

During this phase the level of the certification effort must be defined, and the requirements that affect the system must be determined. The DITSCAP calls for four different levels of certification. See Table C3.T8 of the DoD 5200.40-M.

- **Level 1: Minimum Security Checklist.** Requires completion of the minimum security checklist. The system user or an independent certifier may complete the checklist. This required checklist can be found in Appendix 2 of DoD 8510.1-M, the DITSCAP Application Document.
- **Level 2: Minimum Analysis.** Requires completion of the minimum security checklist and independent certification analysis as defined in the verification and validation phases.
- **Level 3: Detailed Analysis.** Requires completion of the minimum security checklist and more in-depth, independent analysis as defined in the verification and validation phases.
- **Level 4: Extensive Analysis.** Requires completion of the minimum securi-



ty checklist and the most extensive independent analysis as defined in the verification and validation phases.

To determine the required analysis level, refer to Table C3.T9 (System Characteristics) of the DITSCAP Application Manual 8510-1.M (Figure 1). Select the alternative for each of the characteristics that describe

1.M. This brings to light an interesting point.

Table C3.T10 shows the areas of possible contention from using the DITSCAP. From the table we see that the areas between 12 - 16, 24 - 32, and 38 - 44 overlap. This means that either a level one or two, level two or three, or level three or four certification could be required if the total points from table C3.T9

fall into one of those ranges. This is where the “negotiation” aspect of the DITSCAP enters in play. The DAA, certifier, PM, and user representative must collectively agree on the level of effort to be expended on the certification. This is normally accomplished with a minimal amount of bloodshed, and the final decision rests with the DAA, as the DAA will be the official responsible of accepting the risk.

Requirements Traceability Matrix (RTM)

Task 1-5 of the DITSCAP requires the determining of the system’s security requirements. This includes the requirements of the DITSCAP, Army Regulation 380-19,⁴ DISC4 policy memos, patches to the operating system or applications, the system SOPs, and any other requirements that apply to the system. The proponents, specifically the security engineer and the certification team, must analyze the directives and security requisites to determine the applicable security requirements that apply to the system. They will normally take a section of a directive and parse it into a basic security requirements

Characteristic	Alternatives and Weights	Weight
Interfacing Mode	Benign (w= 0), Passive (w= 2), Active (w= 6)	
Processing Mode	Dedicated (w= 1), System High (w= 2), Compartmented (w= 5), Multilevel (w= 8)	
Attribution Mode	None (w= 0), Rudimentary (w= 1), Selected (w= 3) Comprehensive (w= 6)	
Mission-Reliance	None (w= 0), Cursory (w= 1), Partial (w= 3), Total (w= 7)	
Availability	Reasonable (w= 1), Soon (w= 2), ASAP (w= 4) Immediate (w= 7)	
Integrity	Not-applicable (w= 0), Approximate (w= 3), Exact (w= 6)	
Information Categories	Unclassified (w= 1), Sensitive (w= 2), Confidential (w= 3), Secret (w= 5), Top Secret (w= 6), Compartmented/ Special Access Classified (w= 8)	
	Total of all weights.	

Figure 1. Table C3.T9, System Characteristics

the system. Each characteristic has an assigned weight, which is entered in the right column. The total of these weights is used to determine the appropriate certification level.

Table C3.T11 (right) shows an example of a completed System Characteristics table. From this, we see that the system had a total of 27 points.

Based on the total weights calculated, the next step is to select the certification level from table C3.T10 of the DITSCAP 8510-

Characteristic	Alternative	Weight
Interfacing Mode	Active	6
Processing Mode	System High	2
Attribution Mode	Basic	3
Mission-Reliance	Total	7
Availability	ASAP	4
Integrity	Approximate	3
Information	Sensitive	2
	Total of all weights	27

Figure 2. Table C3.T11, Certification Level Example

Certification Level	Weight
Level 1	If the total of the weighing factors in Table 3-1 are < 16
Level 2	If the total of the weighing factors in Table 3-1 are 12-32
Level 3	If the total of the weighing factors in Table 3-1 are 24-44
Level 4	If the total of the weighing factors in Table 3-1 are 38-50

Figure 3. Table C3.T10, DITSCAP Levels of Certification

statement. The security requirements will then be entered into the RTM to support the remainder of the C&A effort.

In the example below the matrix shows the “Source Document,” or regulatory requirement, and the specific paragraph of the requirement that is to be tested.

A spreadsheet format serves well as an RTM, and a comment block may be added to supply more specific details. The RTM follows the requirements through the System Security Requirements Specification (SSRS), and shows the specific paragraph in the Security Test and Evaluation (ST&E) procedure where the requirement is actually tested. The “Evaluation Method” column indicates the type of assessment made—DITSCAP uses I= Interview; D= Document review; T= Test; and O= Observation. A legend explaining these methods may be provided within the spreadsheet as well. The next block shows whether the requirement was met or not. The certifier uses the RTM to follow the progress of the certification effort throughout the entire process. Moreover, at the completion of the certification it provides a handy overview of the entire effort. The RTM

makes it easy to see at a glance which requirements were either met or not.

At the end of the first phase, the proponents have an understanding of exactly what resources the certification process will require. The level of certification has been negotiated, as have the requirements that will

Source Document	Paragraph	SSRS Reference	Certification Procedure Ref.	Evaluation Method	Met	Not Met
AR 380-19	2-3a(2)	2.2.1.1	4.2.1.3.1	I	X	
AR 380-19	2-14i	2.2.2.5	4.2.2.3.9	O	X	
AR 380-19	2-14h	2.2.2.13	4.2.2.3.21	D	X	
AR 380-19	2-24e	2.2.1.9	4.2.1.3.13	T		X

Figure 4. Requirements Traceability Matrix

be tested or verified during phase two. At the end of this phase, the proponents sign the System Security Authorization Agreement (SSAA), meaning that they all agree to fulfill these requirements.

Phase 2: Verification

The major occurrences that take place during this phase are—

The System Security Authorization Agreement (SSAA) is refined. During this phase, the SSAA is being updated as changes occur. It is important that all of the proponents

are made aware of any changes made to the system, because any change can affect the scope of the C&A effort. This is a good example of why some organizations in the C&A business fail to complete the certification process. They may be under the impression that theirs is a limited role, while the exact opposite is true. The certifier and the team must be actively involved in each event that occurs throughout the entire process.

The system is developed.

As the system is developed it is likely that changes will also occur that may impact the C&A process. It is possible that significant changes will even change the certification level itself. It is also important to remember that the requirements of the SSAA are followed throughout

the life cycle of the system. As the size and complexity of the system under development changes, so will the security requirements and thus the C&A effort.

The certification process is analyzed to ensure that it is sufficient.

Because of the changes that have been made to the system, it is necessary to evaluate the security requirements as well to insure their adequacy. This evaluation may lead to the introduction of new or more stringent requirements, or it may necessitate the removal of some of the require-



ments decided upon in Phase 1. Table C4.T1 of the DITSCAP application manual⁵ defines seven certification tasks to be conducted during this phase.

1. System Architecture Analysis
2. Software Design Analysis
3. Network Connection Rule Compliance Analysis
4. Integrity Analysis of Integrated Products
5. Life Cycle Management Analysis
6. Security Requirements Validation Procedures Preparation
7. Vulnerability Assessment

The system is ready. Before entering the actual Validation Phase (Phase 3) the determination is made that the system is ready to be certified. This means that the system is deemed ready for testing of the fully integrated system and its environment, both hardware and software. The system has been evaluated at each step of its development, and any discrepancies identified by the certification team are brought to the attention of the PM, DAA, and user representative so that corrections or modifications may be made.

Any additional resource requirements are reported to the DAA. These additional resources may be required because of a significant change to the scope of the certification effort. Even seemingly insignificant changes to the system design during this phase may require a much more stringent approach to the certification process.

Phase 3: Validation

This is the phase that most people think of when they think

of certification, and that which causes the most confusion to those with doubtful credentials. It is imperative that the certifier and certification team have been active throughout the entire process, and not just this single phase. The certifier and certification team have been instrumental in getting the process to this point, and have provided critical input as to the level of certification, the requirements to be leveled against the system, and in the overseeing of the system development. Now the certifier and certification team have the lead in the C&A effort.

System Test and Evaluation (ST&E).

At the heart of this phase lies the ST&E procedure, a detailed description of the testing of security features to be performed during development in its fielded environment in support of certification. It describes the specific requirement (referenced to the RTM), states the purpose of the test, and delineates the criteria for success. Given the variance and complexity in systems, it is impossible at this time for one set of requirements to effectively fulfill these criteria. Exercise caution when faced with claims that a single tool can do this job – one size does not fit all! The DoD application manual provides an example of the format for each of these test procedures as shown below (comments are italicized)—

1.0 (*Security Policy, or other heading for the major functional area under test*)

1.1 RTM# (*reference to the specific requirement in the RTM*)

Source: (*AR 380-19, Orange Book, etc.*)

1.1.1 Requirement to be tested—*The actual verbiage from the source*

1.1.2 Test Objective (Purpose)—*The reason that this specific test is being conducted*

1.1.3 Test Method (Inspection, Test, or Analysis)—*(Inspection, test, evaluate, demonstration; or: I= Interview; D = Document review; T = Test; and O = Observation)*

1.1.4 Test Scenario (Test Setup)—*A description of any requirements needed to conduct a test, such as setting up user accounts, or test equipment*

1.1.5 Test Procedures—*An exact, detailed explanation of how the test was conducted. This area must contain a detailed, step-by-step list of exactly how the requirement was tested so that the results can be duplicated*

1.1.6 Expected Results—*The expected outcome of the test*

1.1.7 Actual Results—*The actual result of the test. May be "As Expected," if the test passed*

1.1.8 Overall Results/Conclusions— Met Not Met
Whether or not the requirement was met

1.1.9 Comments—*Any comments that the certification team feels necessary to explain the result obtained goes here*

1.1.10 Date Tested, Tested By.
It is important that the person actually conducting the test fill this out when the test is performed. An actual certification will usually have several hundred of these procedures, and this is how it is determined that the test was actually performed.

Other testing areas required under the DITSCAP are penetration testing, verification of TEMPEST compliance (if required), verification of communications security (COMSEC) (if required), a system manage-

ment analysis, a site accreditation survey, an evaluation of the contingency plan, and a risk management review. Also, in most cases a review of the documents listed below is also required. These documents are generally received from the security engineer—

- System Design Plan (SDP)
- Threat Description
- Security Policy (includes system, network, & physical policies)
- Configuration Management Plan (CMP)
- Certification Plan (with certifier)
- Continuity of Operations Plan (COOP)
- System Security Requirements Specification (SSRS - developed with input from the certifier)
- Security Training & Awareness Plan
- Trusted Facilities Manual (TFM)
- Security Features Users Guide (SFUG)
- Incident Response Plan

The certification team works closely with the security engineer and system engineer throughout this phase, as well as throughout the entire process. The security engineer and the certifier maintain a close relationship during the C&A process so that problems may be identified and resolved as soon as possible. It is important that the security engineer be made aware of any extremely high risks as soon as they are identified so they can be mitigated.

Additional Documents Produced

In addition to the ST&E procedures, the certification team must also provide the following documents: Risk Assessment

Report (RAR—previously known as the Security Risk Management Review), Certification Evaluation Report (CER), and the Certification Statement. Each of these documents is discussed below.

Certification Evaluation Report (CER)

The CER contains the “raw” results of the certification testing (ST&E) and forms the foundation for certification. It presents the overall security test philosophy, the detailed ST&E procedures, and the test results with comments from the testers.

The number of attachments to the CER depends on the system’s complexity. For instance, they can be organized by function and have one attachment for routers, one for terminal servers, one for print servers, one for E-mail servers, etc. Or, they might be organized by equipment and have one for Windows NT servers, one for Windows 95 platforms, one for CISCO devices, etc.

There may also be a separate section showing the actual results from any automated scanning tools that were used on the system, and one providing the results of the Site Accreditation Survey.

Risk Assessment Report (RAR)

The DITSCAP calls for a document that provides an analysis of the ST&E failures. This document includes an examination of the threats, vulnerabilities and the resulting risks to the system. In this document each requirement that was not met during the ST&E is viewed as a vulnerability and assigned a risk

continued on page 22

level. The associated risk may be classified as either extremely low, low, moderate, high, or extremely high. This classification is determined by the certification team, and is discussed with the security engineer before a final determination is made. For each risk that is extremely high, this document describes the security weakness and explains why it constitutes vulnerability. Fixes (enhanced or additional countermeasures) are suggested, along with an explanation of how they would reduce the risk. “Initial risk” (as is) and “residual risk” (with the additional countermeasures) are estimated.

Certification Statement

The Certification Statement is the Certification Authority’s report to the DAA on the results of the certification testing. It includes a recommendation to either accredit the system, or not. It may recommend an Interim Approval to Operate (IATO) for up to six months while “High” or “Moderate” risks are being fixed.⁶ The Certification Statement is prepared by the Certifying Agent, and is signed by both the Certification Agent and the certifier. The Certification Statement will contain one of the following recommendations:

- **Full Accreditation**—The system is approved to operate with acceptable risk in the intended environment as stated in the SSAA.
- **Interim Approval to Operate (IATO)**—The system contains unacceptable long term risk but mission criticality mandates the system become operational. Use of the IATO requires a return

to Phase 1 to negotiate accepted solutions, schedules, necessary security activities, and milestones. After the six-month period, those risks will be looked at again, and the threat to the system reassessed. Before any IATO may be issued, Phase 2 and 3 activities must be completed and appropriately documented. This ensures the repeatability of the process.

- **Disapprove Accreditation**—The system contains extremely high risks. The liability is too great to allow the system to be operational. This type of recommendation requires a return to Phase 1 to renegotiate previously accepted solutions, necessary security activities, and milestones. The system must complete Phases 2 and 3. Again, as stated above, this ensures repeatability in the process. If the DITSCAP process is rigorously followed by competent security experts it is unlikely that a recommendation to disapprove accreditation should ever be made.

Phase 4: Post Accreditation

Phase 4 contains process activities necessary to operate and manage the system so that it will maintain an acceptable level of residual risk. It begins after the system has been integrated into the operational computing environment and accredited, and continues throughout the life of the system. It is the responsibility of the Information System Security Officers (ISSO), the DAA, and system operators and administrators to maintain the security posture of

the system. The claim of some organizations to make the re-accreditation process easier for their customers can be misleading, as the role of the certifier is somewhat limited. Army Regulation 380-19 requires re-accreditations within three months following any event below—

- Addition or replacement of a major component or a significant part of a major system
- A change in classification level of information processed
- A change in security mode of operation
- A significant change to the operating system or executive software
- A breach of security, violation of system integrity, or any unusual situation that appears to invalidate the accreditation
- A significant change to the physical structure housing the AIS that could affect the physical security described in the accreditation
- The passage of 3 years since the effective date of the existing accreditation
- A significant change to the threat that could affect Army systems
- A significant change to the availability of safeguards
- A significant change to the user population

AR 380-19 is very specific as to what must be accomplished, and even the timeframe in which re-accreditation must be accomplished. Re-accreditation will include the same steps accomplished for the original accreditation; however, those portions of the documentation that are still valid need not be updated. Therefore, as long as there

continued on page 26

ATM Intrusion Detection Systems *continued*

continued from page 11

streams architecture for the OC-3 IDSs.

The multiprocessing capabilities have not fully been exploited in the currently fielded IDSs. Additional effort needs to be expended to optimize the SMP architecture. One area that could benefit greatly from further SMP refinement is the area of near real-time processes. A goal of the HPCMP is to implement a near real-time IDS capability; to achieve this further optimization of the SMP architecture will be critical.

Finally, currency with the most recent JIDS release is critical to support issues. During the development of the ATM IDS, enhancements were made to the standard JIDS code. The ATM IDS code must merge with the standard version and remain current in the JIDS update process to be fully supported.

Mr. Joseph Molnar is an Information System Security Officer for the High Performance Computing Modernization Program. He earned his B.A. from Washington & Jefferson College in 1981 and his M. S. from The Pennsylvania State University. Both degrees were in physics. He may be reached at molnar@hpcmo.hpc.mil.

continued from page 22

were no changes to the TFM, SFUG, or any of the other documentation, there is no need to look at them again.

It is also a good idea to conduct on-site interviews to ensure that the security training and awareness program works, to conduct scans of the system, and to take another look at the minimum security checklist. The team will probably want to conduct spot checks of previously tested procedures on a random basis as well.

Conclusion

By now you can see that the C&A process, which may initially seem complex, has an underlying logic. It's not all smoke and mirrors—indeed, the flexibility built in to this process helps to ensure its success. Modern-day networks are inherently heterogenous, complex and ever changing⁷ and even after a system has been certified it is still necessary to maintain that level of security. The virtual and physical assets involved normally contain sensitive information, and if shared, create great national security risks. If the DAA, PM, user representative, ISSO, and system administrators all do their jobs, then re-accreditation after three years will be much easier, and the system will also be more secure throughout its entire life-cycle. An agency must take an informed approach to security certification and accreditation to preserve the public trust in their ability to leverage information technology, while avoiding unintended consequences.

For more information on Certification and Accreditation, visit one of these Web sites—

- https://www.isec-sig.army.mil/isectech/teal/tealframe.cfm?ski_ll=secucert&foldername=IE
- <http://www.isec-tech.hqisec.army.mil/isectech/index.htm>
- <https://iase.disa.mil/ditscap.html>
- <http://www.p-and-e.com/documents/DITSCAP.pdf>

Mr. John Kimbell has worked in the computer industry for over 30 years in a wide variety of positions, including the engineering of and modification to secure digital message switching centers, local and wide area networks, and a variety of secure communications systems. He has certified and assisted in the certification of numerous DoD and Army systems, and is presently the Critical Skills Expert in security certification for the United States Army Information Systems Engineering Command (USAISEC) at Fort Huachuca, Arizona. Mr. Kimbell holds a B.S. degree in Computer Science from Chapman University, and a M.S. in Information Systems Engineering from Western International University. He may be reached at kimbellj@HQISEC.Army.mil.

Ms. Marjorie Walrath is a technical editor assigned to USAISEC, Fort Huachuca, Arizona. She is currently at work on a bachelor's degree in communications.

Endnotes

1. Kuzniar, Paul, *Government from the View of Business*, Government Executive, April 2000, p. 97
2. U.S. Department of Agriculture *Inspection and Grading* [on line], <http://www.fsis.usda.gov/oa/pubs/ingrade.htm> August 1998
3. DoD 5200.28 Standard, Department of Defense Trusted Computer System Evaluation Criteria, December, 1985
4. Army Publication & Printing Command, Information Systems Security AR 380-19, sec.2.3, March 1998, http://books.usapa.belvoir.army.mil/cgi-bin/bookmgr/BOOKS/R380_19
5. DoD Application Manual 8510.1-M
6. AR 380-19, ch.3 sec. 3.10
7. Casti, John I. *Would-be Worlds: How Simulation is Changing the Frontiers of Science*, John Wiley & Sons, Inc., 1997, p.x