

Information Systems Security Lifecycle Management

Maintaining the security posture of an information system from its conception to retirement through the integration of Information Systems Security Engineering and sound information assurance practices



Introduction

With continued emphasis on Information Assurance (IA) and the secure management of Information and Information Systems by the Department of Defense (DoD), users of these information systems must assess the most efficient and effective means of applying these practices. Information Systems Security Lifecycle Management (ISSLM) streamlines the steps of the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), enabling users to ensure that the appropriate protocols are implemented during design efforts and maintained throughout the system's use and decommission.

The Business Challenge

Planning and designing a secure solution that implements ISSLM to enhance the government's ability to perform DIACAP is a challenge. Even more challenging is giving the decision-makers in the acquisition process the justification, cost savings, and rationale for pursuing a solution like this from the vendor. If the federal government cannot see the benefits from the solution, then they will not fund it. Typically, four groups emerge in the development and management of a system through its lifecycle (see Figure 1.1).

During acquisition, program managers lack the support or the training to implement the guidance given by the federal government or DoD regarding Information Assurance. Most proposals that are currently developed have language supporting these efforts, but rarely are the Information Assurance requirements correctly understood or vetted by the vendors providing the solution. An example of the typical requirement language for Information Assurance support on a DoD project follows:

All COTS/GOTS must conform to NSTISSP No 11. National Policy Governing the Acquisition of Information Assurance (IA) and IA enabled technology products as of 1 July 2002, must

TCS TeleCommunication
Systems
Enabling Convergent Technologies®

275 West Street
Annapolis, MD 21041
410.263.7616
888.772.7911
410.263.7617 (fax)
www.telecomsys.com

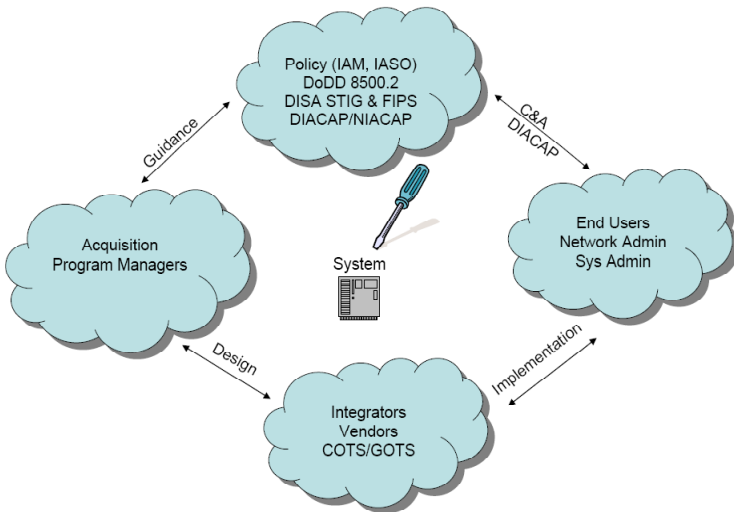


Figure 1.1
Information Systems Management
Lifecycle

be evaluated/validation by International Common Criteria Mutual Recognition, NIAP Evaluation and Validation Program (CCEVS), NIST FIPS validation program. All GOTS IA or IA enabled products must be evaluated by NSA or an NSA approved process. (Guidance DOD Directive 8500.1 – 24 OCT 2002, DOD Instruction 8500.2 – 12 FEB 2003). DoD Information Assurance Certification and Accreditation Process (DIACAP) support will be provided by the vendor.

Vendors must learn to communicate with the customer the need for full ISSLM support from an IA perspective in order to achieve their objective with DIACAP. Problems occur from a lack of understanding among all parties involved in the sales and proposal effort. Even if vendors do not have the capabilities to provide full ISSLM support, it still must be a consideration by the program manager in development of the information system.

In communication with the customer to support IA objectives, the sales staff needs to be familiar with the regulations that support such reasoning. The two most important regulations concerning IA during acquisition are DoD Directive 8500.1 Information Assurance, “Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems”, and DoD Instruction 8510.01 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), outlined by Figure 1.2.

General acquisition regulations such as DoDD 5000.1, “The Defense Acquisition System,” define the need for Information Assurance from a higher level as directed by FISMA (Federal Information Security Management Act). This is the extent to which those involved in the business process need to be familiar. When referring to regulations which are more technical in nature, such as FIPS 140-2 and DoDI 8500.2, which are required by DIACAP and DoDD 8500.1, sales personnel should refer to an IA Engineer when questions arise. The customer is required to provide a means for IA, and is not tied to any one avenue of approach for solving the IA problem.

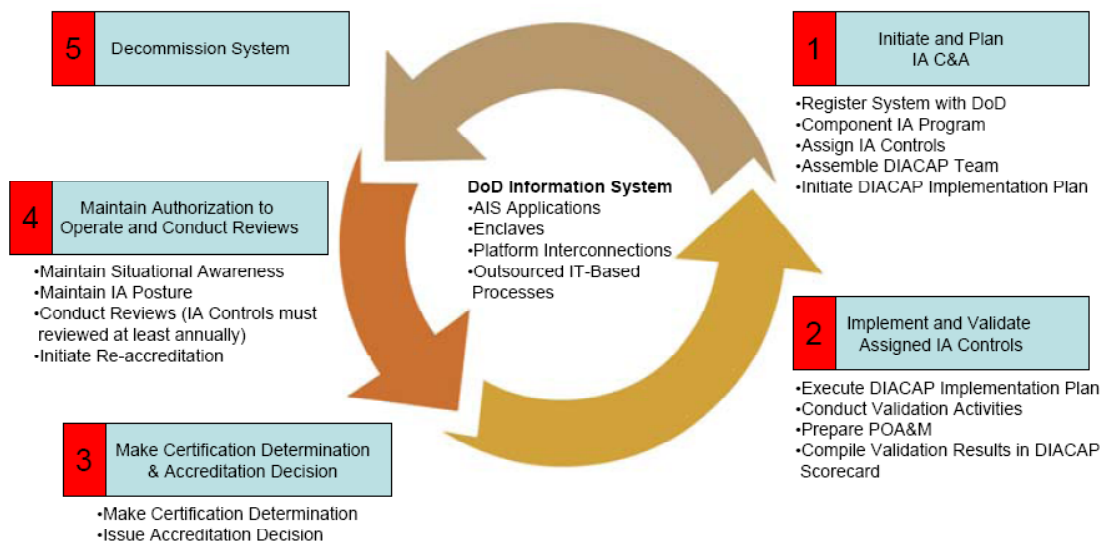


Figure 1.2
DoD Instruction 8510.01 Department of Defense Information
Assurance Certification and Accreditation Process

Once educated on the process, the sales staff works with the customer to address these needs by focusing beyond the required regulations to solutions that enhance the quality of services and reduce costs for the government. The other groups that are involved with the systems security during its lifecycle are continually left out of the acquisition process to the detriment of the system's development. Users and certification and accreditation (C&A) personnel must be brought into the proposal process to ensure that their operational and security requirements are addressed.

The Current Landscape

Currently IA is being applied in an unstructured fashion throughout the DoD. Some components are further along than others in their transition from DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process) to DIACAP, but the determining factors seem to be funding and the local Command's emphasis on IA. Below are some of the prevalent problems in the Information Systems Security Lifecycle of many information systems throughout DoD:

1. Systems are designed without IA as a consideration, therefore undermining the government's ability to administer proper security.
2. IA is rarely considered prior to an information systems procurement, which prevents the local IAM (Information Assurance Manager) from acquiring knowledge of available new systems.
3. ST&E's (Security Test and Evaluation) are not conducted correctly or to any known standard.
4. C&A (Certification and Accreditation) documentation does not accurately reflect the system it is assessing.
5. Accreditations are not properly maintained as the systems change due to a lack of Configuration Control Management.
6. IAVM and other updates for STAMIS (Stand-Alone Management Information Systems) are not maintained.

Information systems are currently designed with no consideration for IA. This happens due to the miscommunication and lack of understanding of IA by the vendor and government when developing system requirements. During these initial stages of development, operational aspects and shortcuts may trump common security practices. The result is a system that is not only insecure, but does not adhere to many of the policies that DoD information systems must follow.

The problem is compounded once the Information Systems is delivered to the customer where the local IAM (Information Assurance Manager) has no prior

knowledge of the system or its development. For a variety of reasons, such as a shortage in funding, staffing or understanding of a complex system, IA is not implemented on the system in a timely manner. If possible, the IAM has an ST&E done, but commonly with no guidance or standard. Personnel who are not qualified to analyze reports or understand the complexity of the system are sent to run a Retina scan. The scanner not only picks up false positives and negatives, but misses many vulnerabilities that can only be found through a manual inspection of the system.

As with any other process, garbage in, garbage out; and this is what happens with the C&A process. Continuing to follow a broken process for administering IA to the system, the erroneous findings from the ST&E are incorporated into the DITSCAP or DIACAP documentation. The results neither reflect the true security posture or design of the system whether good or bad, potentially leaving the customer's system open for attack and creating a false sense of security.

Once the initial C&A has been completed, systems are normally left alone. Configuration management for systems inside the DoD is rarely accomplished in a manner that maintains the security posture of the systems or updates the DIACAP when changes are made. This thwarts the government's ability to maintain the security posture, systems updates, and configuration changes. For STAMIS (Stand Alone Management Information Systems) the problem is usually worse due to the nature of their isolation and not being managed by any remote process such as Active Directory. When administering IAVM (Information Assurance Vulnerability Management), it creates an environment that is almost impossible to maintain. The IAO (Information Assurance Officer) generally takes care of the low hanging fruit (i.e. laptops, desktops, exchange server), but this leaves many critical systems (which are usually STAMIS) wide open and unmanaged across the network.

This scenario is dependent upon the organization, many of which do maintain a good IA posture for all systems; however, this seems to be the exception rather than the standard.

Technical Challenges

There are many technical challenges involved with administering IA for the systems described in the previous section. At times, the challenges come not from a mismanaged IA Program, but from the operational nature of the system.

For systems that were not designed with IA in mind, there are technical challenges when trying to administer security to these systems. Some of the technical issues that may arise include the following:

1. Lack of trained personnel
2. No tools to administer security
3. Remote administration not possible

Lack of trained personnel is a problem that most organizations have when applying IA across their networks. This limits the ability to manage and update systems of various complexities. Obviously when un-trained staff are administering security, it may leave many holes across the network, and compromise the organization's security from not just a single system, but even from an architectural standpoint. Without the proper tool sets, even experienced personnel find it difficult to properly manage the security of their networks and systems. Personnel just don't have the time required to manually inspect significant numbers of systems, which is why tool sets are created. Other times, systems must be checked remotely, with tools scanning them across the network. However, caution must be used when applying tools against systems for the first time, because a combination of lack of experience and running inappropriate tool sets, or testing for the first time, can and often does break the systems, rendering them inoperable. Occasionally, remote administration may not be possible, and the organization may not have access to the system, or lack the expertise to automate or manually apply procedures to update and manage the system.

Current Approaches and Limitations

Currently there is no approach for managing systems through the entire Lifecycle, with the exception of entering them into an AVTR (Asset Vulnerability and Track Resource), which merely tracks the system and its current status. Most organizations try to administer security management for IA purposes remotely. This is normally accomplished for common systems such as laptops, desktops or servers using applications like Active Directory, Hercules, SMS or WSUS to manage and update systems. This works well in these environments for common systems, but as soon as the complexity level or operational nature of the systems change, they are left out of the loop. As discussed in the previous section, many times the personnel may not be trained on the system, or lack the technical expertise to maintain the system. This creates an environment where systems have at

times been left for months or even years without any administration from an IA perspective. This can be compounded with the operational nature of a system that cannot be administered remotely, such as a STAMIS, but administrators on the ground are generally not trained in IA, so they do not update the systems.

Recommended Approach

To address this problem, a methodology must be created that is specific in addressing those important areas of Information Assurance that maintain the security posture of the system throughout the system's lifecycle. This creates an Information Systems Security Lifecycle Process by addressing the following areas:

1. Ensuring that all aspects of IA are addressed in the SOW.
2. Incorporation of Information Systems Security Engineering into the design of the information system.
3. Ensure that the CONOPS of the system does not interfere with the security of the system.
4. Ensure that DIACAP is incorporated into the Information Systems Security Lifecycle Process.
5. Ensure qualified personnel with the appropriate tool sets are tasked to work on the system.
6. Ensure that Configuration Control Management is incorporated into the Information Systems Security Lifecycle Process.
7. Maintain and update the systems according to DISA and Organizational Policies and Procedures.

A methodology must be established due to the fact that all of the areas listed above generally are tasked to different parties throughout the life of a system. Tying them together to create a seamless platform from which to administer security will enhance the system's security posture.

Implementation Considerations

In creating a methodology to address the issues listed above, one must address several different aspects that may hinder the ability for the methodology to work correctly. Scalability is one important factor that must be addressed. Scalability refers to both the size and complexity of the system. An increase in size or complexity leads to a concomitant increase in the effort involved in applying any particular security methodology. The security methodology should work for a single laptop running Windows XP, a deployable kit containing anything from WiMAX to satellite technology, or a complete network for an organization as the standard template for applying Information Systems Security Lifecycle Management.

It is very important as well that the methodology work well throughout DoD and Federal Government while maintaining applicability to all components and commands. Whether Army or Navy, with different acronyms and different regulations such as AR 25-2 Information Assurance, the methodology must have the ability to work for all and apply the inputs from data obtained into the DIACAP or NIACAP process where applicable.

TCS Information Systems Security Lifecycle Management Methodology

Telecommunications Systems, Inc. (TCS) provides a methodology suitable to any information system or organization to maintain the security posture of systems throughout the lifecycle in order to enable proper C&A. While developing the methodology, TCS focused on the key areas that enable a more comprehensive way to enable the end user to apply security:

1. **KIS: Keep it Simple**, one of the most important aspects in enabling the end user to accomplish their security objectives.
2. **Cost**: Reducing cost by minimizing the time spent in design and maintenance of the system.
3. **Empowering the end user**: Giving the user the ability to meet today's security demands. Through the ISSLM, TCS provides detailed instruction sets to direct users and systems administrators on how to implement and maintain the security posture of a system.
4. **Enhance security professionals abilities**: Though security professionals may be an expert in security, they may not fully understand the system or Concept of Operations (CONOPS) for the system. TCS provides detailed analysis of the system and CONOPS to facilitate this.
5. **Functionality**: TCS' ISSLM can be used in any environment and provides the data that any authorized interested party would find useful and easy to navigate.
6. **Reproducible**: May be easily replicated with various projects.
7. **Accurate and applicable**: For C&A purposes, being accurate is paramount, while maintaining applicability to the system is a value-add.

The methodology is comprised of several different elements:

1. Assembling a team of IA engineers and analysts with the appropriate skill sets to meet the demands of the project.
2. If possible, ensuring that all IA requirements for

the management of the system through the entire lifecycle are addressed with the customer and incorporated into the initial SOW (statement of work) for the system.

3. Incorporating sound Information Systems Security Engineering into the design of the system.
4. Verifying the CONOPS (Concept of Operations) does not interfere with the security of the system.
5. Initiating DIACAP activities during the design of the system.
6. Completing a thorough ST&E of the product prior to delivery of the system for incorporation into DIACAP.
7. Integration of all inputs from previous efforts (ST&E & ISSE) into the TCS Security Documentation, Implementation and Maintenance Process (SDIM).
8. Providing an appropriate means of maintaining, updating, and providing configuration control management to the security posture of the system throughout the Lifecycle of the system with SDIM.

TCS Information Assurance Project Team

The TCS Information Assurance Project Team provides professional Information Assurance (IA) support with staff that meet or exceed the training and education requirements outlined in DoD 8570.1-M (Information Assurance Workforce Improvement Program). Team Leads designated for a project will have education that exceeds prerequisites to include but not limited to Certified Information System Security Professionals (CISSP), National Security Agency (NSA) Information Security Assessment and Evaluation Methodologies (IAM/IEM), and Information Operations expertise. TCS also ensures that team members have expertise in the appropriate C&A method used for each particular organization whether it be DIACAP (Department of Defense Information Assurance Certification and Accreditation Process) or NIACAP (National Information Assurance Certification and Accreditation Process). The rest of the team consists of analysts and engineers who have expertise on the individual devices that comprise the system.

Decomposition of Customer Requirements in SOW

During the analysis of an RFP (Request for Proposal) by TCS, sales personnel and a designated IA Engineer vet all IA requirements applicable to the system to ensure the best possible solution is developed. If the SOW does not call for a full solution, TCS can later provide additional services as an add-on to deliver the best IA

solution for the system. Ensuring that IA is addressed in the contract provides a way to manage the IA through the entire ISSLM.

Information Systems Security Engineering Incorporation

The incorporation of sound ISSE (Information Systems Security Engineering) into the design provides a secure system to DISA (Defense Information Systems Agency) and other federal agencies standards. IA engineers work with systems engineers, integrators, and subcontractors to ensure all stages of development have ISSE incorporated. During the developmental stages, the TCS ISSE methodology follows five steps.

1. TCS focuses on devices that comprise the system, ensuring approved systems (i.e. routers or switches) are utilized, approved encryption modules are FIPS 140-2 compliant (i.e. Air Fortress, TACLANE), and vendors supply software updates for compliance (i.e., enabling GUI management interfaces to use TLS/SSL instead of generic HTTP).
2. TCS then studies the overall architecture to ensure it is designed in a secure manner. TCS examines how the system communicates internally and externally, where encryption needs to be used. Proper access control lists and VLANs are created on the router and switches to manage traffic.
3. TCS then applies all DISA STIG (Security Technical Implementation Guides) and IAVA (Information Assurance Vulnerability Alerts) where applicable to the system.
4. TCS documents all security updates, configurations changes and controls to be analyzed in the upcoming ST&E on the system.
5. TCS builds a prototype that will be used for the ST&E effort based on the developmental designs and best assumptions. IA engineers study the system to ensure that impacts from security requirements are limited in their affect to the CONOPS and mission requirements of the system.

Initiating DIACAP Activities

The ISSE efforts, ST&E and SDIM (Security Documentation, Implementation and Maintenance) processes provide a stepping stone in completing Phases I, II and IV of the DIACAP for the ISSLM of the system. These three processes are key in creating and maintaining the different areas of the DIACAP such as:

1. SIP (Systems Identification Profile)
2. Assignment of IA Controls
3. DIP (DIACAP Implementation Plan)
4. Validations of IA Controls

5. DIACAP Scorecard
6. POA&M (Plan of Action and Milestones)
7. Periodic or Quarterly Scans and Assessments
8. Configuration Control Management

ST&E Security Test and Evaluation

Once it is determined that the functionality of the system produces the desired results, a mock system is built for the ST&E effort to validate all security findings that were incorporated. Where possible, a complete lab environment is set up with government interaction and GFE equipment, if available or necessary to complete a proper test of the system. The test lab serves more than the ST&E – such as maintaining the security posture of the system (if designated by contract) for the entire lifecycle by testing and applying new updates, changes to the configurations, and the addition of new equipment.

The Security Test and Evaluation (ST&E) of the system is done against its baseline configuration for deployment using a methodology that focuses on the following:

1. A complete check against appropriate DISA STIGs, best business practices, and applicable scanning/security tools to ensure that systems are implemented in a secure manner.
2. The ability to implement the system in a secure manner using the TCS III Step Implementation Process.
3. Providing data relevant to completing all DIACAP activities for the system.
4. Provide training tools for the end user with example configurations, diagrams and other technical documentation for the devices.
5. Verifying security requirements do not impact the CONOPS and mission requirements of the system.
6. Providing the means to maintain the baseline of the system through the use of the TCS Configuration Management Methodology, based upon the ST&E efforts.

TCS understands that the DISA STIGs can be confusing and in many cases not relevant to the system under evaluation. This process is simplified by combining all relevant SRRs (Security Readiness Reviews) and STIG Checklists (see Figure 1.3) that may pertain to a system and converting them to a unified format. This enables not only those who are familiar with the DISA STIG process to read them, but more importantly, those who are not. Following is an example of the process for converting the STIG vulnerabilities found through this process.

Once the STIG reviews have been completed with a manual check of the system, the appropriate DoD tool sets are used to validate findings. Tool sets commonly

WIR0010 (STIG Ref)	V0008283 (VMS #)	CAT LEVEL	Vulnerability Title			
	8500.2 IA Control:			Applicable Checklists:	Applies to:	
	References:	Usually refers to the STIG that requires the control				
	Vulnerability	This is the description of the vulnerability.				
	Checks (# from checklist)	Checks involved in checking for the vulnerability				
	Fixes	The approved DISA method for correcting found vulnerabilities.				
Color Coded Response	System	Name of the device				
	OPEN:		NOT A FINDING:		NOT REVIEWED:	
	Comments:	Describes the results of the check				

The following is the color coding scheme

	Open: Constitutes a Vulnerability	This means that the vulnerability currently exists on the system and must be documented for approval from the DAA.
	Not a Finding: Implementation Vulnerability	These vulnerabilities will exist once the system has been implemented or fielded. An example would be changing the default passwords and adding user accounts to the system.
	Not a Finding: Potential Vulnerability	These vulnerabilities could exist on a system. They generally consists of controls from the STIG that involve policy or environment variables that cannot be ascertained at this time.
	Not a Finding:	These controls have been verified as compliant to the STIG or other regulation requiring them.
	Not Applicable:	These controls are not applicable to the system.

Figure 1.3
Example of STIG Checklist Requirement

used are Retina Scanner, Nessus, SANS Router Analysis Tool, and the DISA Gold Disk. Findings are incorporated into the checklists with the engineer's comments. If false positives are found, they are noted.

TCS then follows the III Step Implementation Process. This process is unique to TCS and, as indicated with the color coding above, there are three categories:

1. Red: Open. These are findings that constitute a vulnerability that is found on the system. Further, these vulnerabilities cannot be corrected for a variety of reasons, such as: they impact the functionality of the system, the system is not capable of meeting the specified requirement, or the system, though vulnerable, has been mitigated through another means.
2. Orange: These are vulnerabilities that have not been addressed. This is because they are dependant upon the environment in which the system will be placed.

An example would be the use of RADIUS or TACACS on the routers. Naturally in a production environment, the routers cannot be set up for the customer's RADIUS server, nor can passwords be issued to the users. A list of all items that fall into this category is published with step-by-step procedures on how to implement them. This means that any systems or network administrator should be able to implement all these findings and report back to the local Information Assurance Officer on those that either do not apply or cannot be applied.

3. Grey: Policy or other findings that are not critical, but will need to be addressed by the IA official for the system. In most cases TCS would be able to provide assistance or direction for these types of findings.

From these test results, TCS creates the DoDI 8500.2 Crosswalk Matrix to map all related STIG Vulnerabilities to their corresponding Mission Assurance Category Control

for use in the DIACAP which completes inputs needed for Phase I of the process. TCS uses the ST&E process and inputs obtained to maintain a platform from which all the remaining phases of DIACAP will be processed.

The Security Documentation, Implementation and Maintenance Process (SDIM)

The TCS SDIM Process is the best way to create and maintain the security posture of a system. Typically this is done on a quarterly basis with the application delivered in DVD format and maintained with the system, but other means are available such as a central repository to browse through multiple systems. The goal of the SDIM Process is to enable all responsible parties of the system to maintain the security posture and not just the IAM (Information Assurance Manager). As you can see from the screen shot, TCS has created an easy way to navigate the security settings for a system. TCS discusses each section and its importance to the DIACAP and Security Maintenance of the system.

Section 1: Change Management for SDIM DVD

This section contains detailed information about the evolution of the SDIM product. Typically released on a

quarterly basis, the document for each revision lists all sections that have been updated since the last release. This enables a technician to zero in on any changes that may require specific attention. Examples would be an IOS change for network administrators, IAVA maintenance for the ISO, or a modification to the design of the system that requires changes in the DIACAP documentation. Overall, this is a unique system developed by TCS that enables all parties invested in this system to understand what changes are taking place in a timely fashion.

Section 2: Documentation Legend and Instructions

This section (ref Figure 1.3, Example of STIG Checklist Requirement above) is a brief summary of the different checklists or formats used to present the data collected. It enables any user to understand and analyze the information presented to answer any questions they may have about the security posture of the system.

Section 3: Vulnerability Summary Page and Section 4: Checklists and Reports

These sections are broken down by the different categories of the DISA STIG such as Network, XP,

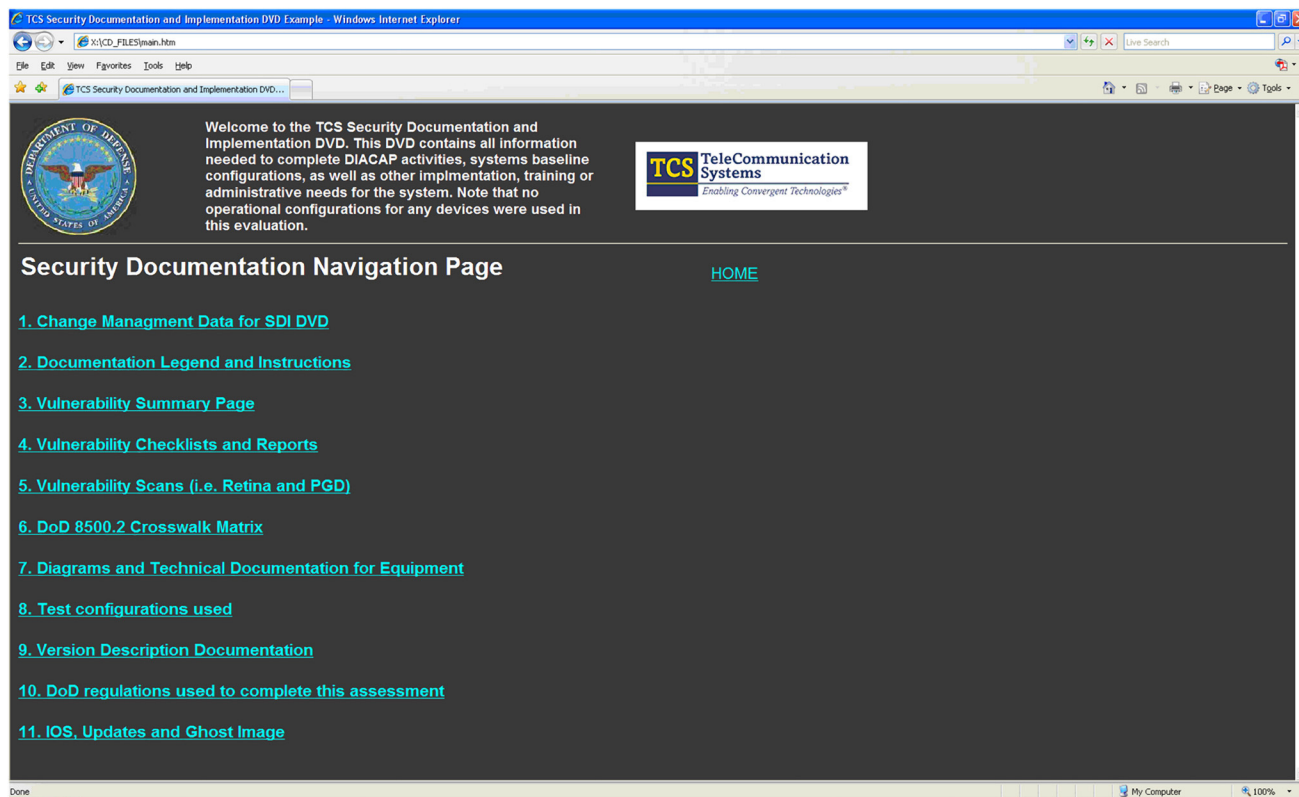


Figure 1.4
Security Documentation Navigation Page

Web Server or VoIP and updated with each version of the SDIM DVD as a version number. For example, every quarterly release will have an additional section with the appropriate version number that lists each checklist run against the system for any new vulnerability that may have been released. The individual checklists are then rolled up to a summary page to enable a view of all vulnerabilities on the system. The Summary Pages are generally designed with an executive view for the decision makers, while the Checklist and Reports Page are designed for analysts and engineers. The checklists are compiled from data obtained manually or through vulnerability assessment tools like Retina Scanner or SANS Router Analysis Tool. The vulnerabilities are broken down as described earlier in the III Step Implementation Process for systems/network administrators to implement a system with little or no help from the local Information System Security Officer. Information Assurance Vulnerability (IAV) updates include Alerts (IAVA), Bulletins (IAVB), and Tech Tips (IAVTT) and are addressed at this time as well. Further, these checklists are used as training aids for technicians in the set up of the system for different environments.

Section 5: Vulnerability Scans Page

Where applicable, systems will have quarterly vulnerability scans run with the appropriate tool. The results are analyzed and any new STIG or IAVA researched to identify applicable countermeasures (patch, fix or meditation/mitigation solution). All data, including the scans will be incorporated into the SDIM (Security Documentation Implementation and Maintenance) DVD or Database for that system giving an operational snapshot of its security posture. This enables TCS to provide IAVA compliance for FISMA and DIACAP related requirements. TCS conducts the test according to the approved TCS Production Information Systems Security Engineering Methodology that was used to create the SDIM, which requires the test bed to be configured according to the approved baseline of the system as laid out in the SDIM to mirror the operational systems/devices being tested. All scans are retained and segregated by version number in the same fashion as the checklists to give a historical view of the security posture. During this quarterly scan, TCS recommends that government representatives be present to alleviate the need for a disinterested third party with regards to the scan results on our own equipment. For systems developed by other vendors, TCS serves as a disinterested third party. Generally these scans are done in a test environment with systems that have no real world data (i.e. no real IP addresses, naming conventions, user names, passwords, or systems locations). Therefore they do not have a classification of secret as most vulnerability scans do. This differs from actual scans of fielded systems because they are based on the baseline of the system, while the configuration of

fielded systems will vary from each location. They help to identify any false positives, or negatives that may exist for remediation purposes. This further enables the scans and configurations to be used as training tools for soldiers when assessing fielded systems.

Section 6: DoDI 8500.2 Crosswalk Matrix and IAVM Compliance/Non-Compliance

For inclusion to the DIACAP, TCS provides the DoDI 8500.2 crosswalk matrix that cross-references any vulnerability found with the appropriate MAC and Sensitivity level. This is included with the quarterly IAVM compliance/non-compliance status for all devices that have been through the ST&E processes and added to the SDIM matrix. Information consists of system type and IAVAs/8500 control which apply and have been mediated or mitigated, or are pending action. A quarterly roll-up of each system is added to the SDIM for each system for configuration management and historical purposes.

Section 7: Diagrams and Technical Documentation

Another benefit to the SDIM is the incorporation of all applicable technical diagrams and documentation that makes up the system. Diagrams include, but are not limited to, Structural, Network Architecture, Wiring, or IP Communications. Technical documentation includes but is not limited to User Manuals, Security Function User Guides (SFUG), or Installation Manuals. This enables the user to have the most current documentation on the system at any given time for training, technical or IA support

Section 8: Test Configurations Used

The test configurations used in the lab are included as a verification of the system's baseline once installed. They are also used as training aids, or as a means to trouble shoot problems that may occur in the field. An example of how the configurations are stored would be the sample router configuration used in the test environment. For each version of the SDIM DVD there is a new copy of the configuration added.

Section 9: Version Description Document

The Version Description Document (VDD) shows the software and hardware versions of all devices that comprise the system. This document changes quarterly to document any software or hardware changes that occur on the system. An example of a device included on the VDD would be Windows XP with a list of all installed applications and their versions (i.e. Symantec 10.1) and all hotfixes or updates installed on the operating system as well. This information is useful in the DIACAP and IAVM process in ensuring the most current software and updates are installed.

Section 10: Regulations

Since TCS checklists are of a proprietary nature to consolidate the view into an easy to read format, references to all related Federal documentation such as DISA STIGs or SRRs are provided. All other regulations used are included with the SDIM for all parties that may have an interest.

Section 11: IOS Updates and Images

In support of IAVM and general systems support, TCS includes all updates, IOS, and systems images that may need to be installed on the systems. On quarterly releases, where possible, updates are automated with step-by-step instructions for each device. With all available updates it gives systems administrators an opportunity to bring a system up to the current standard regardless of the current state. In the event that systems fail, they are used to build systems to a secure state by following instruction sets that have been included with the SDIM DVD.

Synopsis

Through the use of our different processes like the ST&E (Security Test and Evaluation), Ill Step Implementation Process, and the SDIM (Security Documentation, Implementation, and Implementation) Process, managing systems through the ISSLM (Information Systems Security Lifecycle Management) becomes a manageable task. Whether you are updating your information in AVTR (Asset Vulnerability and Track Resource), VMS (Vulnerability Management System), Exacta, eMass or working on any phase of the DIACAP, the TCS ISSLM Process can help you every step of the way.

Contact Information

For more information call us at 1.800.307.9489 or e-mail sales@telecomsys.com. Learn about TCS' products and services at www.telecomsys.com.

Notices

© 2008 TeleCommunication Systems, Inc. All rights reserved. No part of this White Paper, including text, diagrams, or icons, may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording, or otherwise) without the prior written permission of TeleCommunication Systems, Inc.

Note to U.S. Government Users

Documentation related to restricted right - use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraphs (a) through (d) of the Commercial Computer - Restricted Rights clause at FAR 52.227-19 when applicable, or in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013, and in similar clauses in the NASA FAR Supplement.

Information in this document is subject to change without notice. TeleCommunication Systems, Inc. may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you license to these patents, trademarks, copyrights, or other intellectual property. Please send licensing inquiries to: TeleCommunication Systems, Inc., 275 West Street, Annapolis, Maryland, 21401.

DISCLAIMER OF WARRANTY: THIS WHITE PAPER IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, REGARDING THE CONTENTS OF THIS PAPER, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES FOR THE PAPER'S QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE.

Trademark Attributions

Enabling Convergent Technologies is a registered trademark of TeleCommunication Systems, Inc. All rights reserved. All other trademarks, logos and service marks are property of their respective owners.



TCS • 275 West Street, Annapolis, MD 21401 USA • Toll Free: 1.800.307.9489 • Outside US: +1.410.263.7616 • www.telecomsys.com

Copyright © 2009 TeleCommunication Systems, Inc. (TCS). All rights reserved. Enabling Convergent Technologies® is a registered trademark of TCS. All other trademarks are the property of their respective companies. Information subject to change without notice. | NasdaqGM: TSYS | 71509