

Summer 2006

# Secure Configuration tool Suite Initiative

Victor M. Lugo Jr.  
*Regis University*

Follow this and additional works at: <https://epublications.regis.edu/theses>



Part of the [Computer Sciences Commons](#)

---

## Recommended Citation

Lugo, Victor M. Jr., "Secure Configuration tool Suite Initiative" (2006). *All Regis University Theses*. 343.  
<https://epublications.regis.edu/theses/343>

This Thesis - Open Access is brought to you for free and open access by ePublications at Regis University. It has been accepted for inclusion in All Regis University Theses by an authorized administrator of ePublications at Regis University. For more information, please contact [epublications@regis.edu](mailto:epublications@regis.edu).

**Regis University**  
School for Professional Studies Graduate Programs  
**Final Project/Thesis**

**Disclaimer**

Use of the materials available in the Regis University Thesis Collection ("Collection") is limited and restricted to those users who agree to comply with the following terms of use. Regis University reserves the right to deny access to the Collection to any person who violates these terms of use or who seeks to or does alter, avoid or supersede the functional conditions, restrictions and limitations of the Collection.

The site may be used only for lawful purposes. The user is solely responsible for knowing and adhering to any and all applicable laws, rules, and regulations relating or pertaining to use of the Collection.

All content in this Collection is owned by and subject to the exclusive control of Regis University and the authors of the materials. It is available only for research purposes and may not be used in violation of copyright laws or for unlawful purposes. The materials may not be downloaded in whole or in part without permission of the copyright holder or as otherwise authorized in the "fair use" standards of the U.S. copyright laws and regulations.

SECURE CONFIGURATION TOOL SUITE INITIATIVE

DOD's SCTS Initiative

Victor M. Lugo Jr

Regis University

School for Professional Studies

Master of Science in Computer Information Technology

June 20, 2006

Regis University

School for Professional Studies Graduate Programs

MSCIT Program

Graduate Programs Final Project/Thesis

Certification of Authorship of Professional Project Work

Print Student's Name Victor M Lugo Jr

Telephone 717-263-2282 Email victor\_lugo@comcast.net

Date of Submission \_\_\_\_\_ Degree Program MSCIT

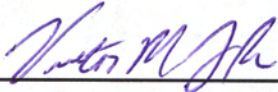
Title of Submission Secure Configuration Tool Suite Initiative

Advisor/Faculty Name Paul Vieira

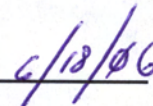
---

Certification of Authorship:

I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for the purpose of partial fulfillment of requirements for the Master of Science in Computer Information Technology Degree Program.



*Student Signature*



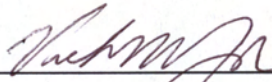
*Date*

Regis University  
 School for Professional Studies Graduate Programs  
 MSCIT Program  
 Graduate Programs Final Project/Thesis  
Authorization to Publish Student Work

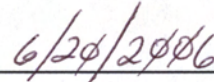
I, Victor M. Lugo Jr, the undersigned student, in the Master of Science in Computer Information Technology Degree Program hereby authorize Regis University to publish through a Regis University owned and maintained web server, the document described below ("Work"). I acknowledge and understand that the Work will be freely available to all users of the World Wide Web under the condition that it can only be used for legitimate, non-commercial academic research and study. I understand that this restriction on use will be contained in a header note on the Regis University web site but will not be otherwise policed or enforced. I understand and acknowledge that under the Family Educational Rights and Privacy Act I have no obligation to release the Work to any party for any purpose. I am authorizing the release of the Work as a voluntary act without any coercion or restraint. On behalf of myself, my heirs, personal representatives and beneficiaries, I do hereby release Regis University, its officers, employees and agents from any claims, causes, causes of action, law suits, claims for injury, defamation, or other damage to me or my family arising out of or resulting from good faith compliance with the provisions of this authorization. This authorization shall be valid and in force until rescinded in writing.

Print Title of Document(s) to be published: \_\_\_\_\_

Secure Configuration Tool Suite Initiative



Student Signature



Date

Check if applicable:

The Work contains private or proprietary information of the following parties and their attached permission is required as well:

Defense Information Systems Agency (DISA) / Public Affairs Officer  
 Name of Organization and/or Authorized Personnel

DoD's SCTS Initiative 4

Regis University  
 School for Professional Studies Graduate Programs  
 MSCIT Program  
 Graduate Programs Final Project/Thesis  
Releasor Authorization to Publish Student Work WWW

I, TERRI STOVER / DISA the undersigned, Deputy Public Affairs Officer  
*Print Name of Company/Organization Representative* *Representative's Title*

on behalf of Defense Information Systems Agency ("Releasor") do hereby authorize  
*Company/Organization Name*  
 Regis University to publish through a Regis University owned and maintained web server, the document described below ("Work") and acknowledges that the Work contains personal or proprietary information of the Releasor. Releasor further acknowledges and understands that the Work will be freely available to all users of the World Wide Web under the condition that it can only be used for legitimate, non-commercial academic research and study but that this restriction on use will be contained in a header note on the Regis University web site but will not otherwise be policed or enforced. This authorization shall be valid and in force until rescinded in writing.

Print Student Name: Victor Lugo

Title(s) of document(s) to be published: Secure Configuration Tool Suite Initiative

BY: TERRI STOVER DATE: 6-7-06  
*Company/Organization Releasor Signature*

**Note: It is the student's responsibility to obtain the necessary release(s) prior to submitting the Final Project for publication. Please print your name and list all applicable documents.**

Regis University  
School for Professional Studies Graduate Programs  
MSCIT Program  
Graduate Programs Final Project/Thesis  
Advisor/Professional Project Faculty Approval Form

Student's Name: Victor M Lugo Jr Program MSCIT

*PLEASE PRINT*

Professional Project Title: Secure Configuration Tool Suite Initiative

*PLEASE PRINT*

Advisor Name Paul Vieira

*PLEASE PRINT*

Project Faculty Name Joseph Gerber

*PLEASE PRINT*

Advisor/Faculty Declaration:

I have advised this student through the Professional Project Process and approve of the final document as acceptable to be submitted as fulfillment of partial completion of requirements for the MSCIT Degree Program.

Project Advisor Approval:

\_\_\_\_\_  
*Original Signature*

\_\_\_\_\_  
*Date*

Degree Chair Approval if:

The student has received project approval from Faculty and has followed due process in the completion of the project and subsequent documentation.

\_\_\_\_\_  
*Original Degree Chair/Designee Signature*

\_\_\_\_\_  
*Date*

## Abstract

Vulnerability identification, remediation, and compliance verification within the Department of Defense (DOD) are currently inconsistent and non-integrated. The Secure Configuration Tool Suite (SCTS) solution should make significant grounds in resolving the DOD deficiency within an Enterprise-wide Information Assurance Vulnerability Management System.

The professional project documented in this paper is a result of a major DOD initiative in support of the SCTS, and is comprised of 2 initiatives: the Secure Configuration Compliance Validation Initiative (SCCVI), which provides vulnerability assessment capability, and the Secure Configuration Remediation Initiative (SCRI), which provides vulnerability remediation capability. As a member of the project installation team the author performed on-site installations as required and directed.

The DOD is a large organization and documenting the entire project would be beyond the scope of this professional project. Therefore, this analysis is based on a smaller scale of the initiative above. The installation of an unclassified baseline model at a pre-selected DOD command and all of its subcomponents will be utilized for this thesis. This installation will eventually be available for all DOD components to use as a lessons-learned tool and as a result these tools will be applied across the DOD Enterprise and should fully integrate IA Vulnerability identification, verification, and reporting; thus making a significant contribution to an Enterprise-wide Information Assurance Vulnerability Management System.

While this project is based on actual events and efforts, in order to keep within the guidelines of non-disclosure outside of the DOD environment, specific names of commands, agencies and locations have been substituted with generic ones.



## **Acknowledgements**

There are so many people to thank for arriving at this point. I like to start off by thanking all the Professors from Regis University who challenged me to think out of the box and provided me the tools necessary to complete this project.

Second, I would like to thank all my fellow students who have inspired me during the last two years with the academic and technical discussions. These discussions contributed significantly to the preparation and completion of this project.

Third, I would like to thank my present employer and the agency I work for. If not for them I would not have had the opportunity to be part of this project.

Finally, my wife and children who sacrificed the last two years and many hours I was unable to spend with them; this was nothing short of a blessing. Without their understanding none of this would have been possible.

## Table of Contents

|   |    |
|---|----|
| List of Tables .....  | 11 |
| List of Figures .....   | 12 |
| Executive Summary .....   | 13 |
| Chapter One .....   | 14 |
| Introduction .....  | 14 |
| IA Enterprise Tools Overview .....                                  | 14 |
| Secure Configuration Compliance Validation Initiative (SCCVI) ..... | 15 |
| Secure Configuration Remediation Initiative (SCRI) .....            | 16 |
| Hypothesis .....  | 17 |
| Purpose of Research .....   | 17 |
| Limitations / Scope .....   | 18 |
| Definition of Terms .....   | 18 |
| Summary .....   | 18 |
| Chapter Two .....   | 19 |
| Overview .....  | 19 |
| Literature Review .....   | 19 |
| What is Known/Unknown about the Project .....                       | 23 |
| Contribution the Project will make to the Field .....               | 24 |
| Chapter Three .....   | 24 |
| Methodology .....   | 24 |
| Specific Procedures .....   | 25 |
| Initiation Phase .....  | 25 |
| Site Survey Phase .....   | 25 |

Installation Phase .....26

Post-Installation Phase .....26

Sustainment Phase.....26

Deliverables ..... 26

Resource Requirements..... 26

Outcome ..... 27

Summary ..... 27

Chapter 4.....28

Project History ..... 28

    How the project was managed .....28

    Changes to project.....29

    Where goals meet.....30

    Findings.....30

Summary of Results ..... 31

Chapter 5.....33

What was learned ..... 33

    Technical: .....33

    Non-Technical:.....34

    What would have been done differently .....34

Possible Future Work..... 35

Conclusions / recommendations ..... 35

Summary ..... 36

Appendix A – SCCVI Site Survey checklist .....37

Appendix B – SCRI Site Survey checklist .....41

Appendix C – Network Diagram of Installation.....53

Appendix D – Acronym Listing .....54

Glossary of Terms.....56

Annotated Bibliography.....58

References.....60

Work Cited.....62

## List of Tables

TABLE 1 SDLC COMPARISON WITH PROJECT PHASES ..... 25

TABLE 5 POST INSTALLATION PHASE: ENTRY AND EXIT CRITERIA ..... 29

TABLE 6 SUSTAINMENT PHASE: ENTRY AND EXIT CRITERIA ..... 29

TABLE 2 INITIATION PHASE: ENTRY AND EXIT CRITERIA..... 28

TABLE 3 SITE SURVEY PHASE: ENTRY AND EXIT CRITERIA ..... 28

TABLE 4 INSTALLATION PHASE: ENTRY AND EXIT CRITERIA ..... 28

# List of Figures

FIGURE 1 NETWORK DIAGRAM OF INSTALLATION..... 53

## Executive Summary

Vulnerability identification, remediation, and compliance verification within Department of Defense (DOD) are currently inconsistent and non-integrated. The requirement to resolve this deficiency was identified by the DOD Enterprise-wide Information Assurance and Computer Network Defense (IA/CND) Solutions Steering Group (ESSG) chaired by a major strategic command. My agency, at the request of this command and in support of National Security goals, purchased from industry; a capability that will assist in the development and deployment of an automated tool that will provide network administrators and security personnel a mechanism for the remediation of vulnerabilities based on DOD instructions. This tool suite, consisting of the Secure Configuration Compliance Validation Initiative (SCCVI) tool and the Secure Configuration Remediation Initiative (SCRI) tool, will be the "Enterprise-wide" solution known as the Secure Configuration Tool Suite (SCTS) across the DOD (Combatant Commands, Intelligence Community (non-Title 50 elements), Services, and DOD Agencies), Coast Guard, National Guard, and the Reserves, hereafter referred to as the "Enterprise." This project covers the installation of these tools at a major Combatant Command and its Sub-Components in an effort to establish a baseline and concept of operations for all subsequent installations to follow.

## Chapter One

### ***Introduction***

In addition to the traditional *Information Assurance* (IA) capabilities provided by my employer, we are also supporting a major *Department of Defense* (DOD) *Combatant Command's* initiative developed and approved by the *Enterprise Solutions Steering Group* (ESSG) of my organization by providing DOD level enterprise-wide solutions for IA.

My employer is the deploying arm for these efforts and we will provide installation support for the *Secure Configuration Tool Suite* (SCTS) Initiative. SCTS is the DOD enterprise-wide solution for vulnerability assessment and vulnerability remediation and is comprised of two initiatives.

The *Secure Configuration Compliance Validation Initiative* (SCCVI) provides vulnerability assessment capability and the *Secure Configuration Remediation Initiative* (SCRI) provides vulnerability remediation capability. These products were purchased from Citadel Security Software, Inc. and eEye Digital Security.

These tools will be applied Enterprise-wide across the DOD, Coast Guard, National Guard, and the Reserves. This capability should fully integrate IA Vulnerability identification, verification, and reporting.

This project is an effort to install the SCTS at a major combatant command to be utilized as the baseline for future installations at other DOD components.

### ***IA Enterprise Tools Overview***

The Secure Configuration Tool Suite (SCTS) is a DOD enterprise-wide solution for vulnerability assessment and vulnerability remediation and is comprised of two initiatives. These initiatives are the Secure Configuration Compliance Validation Initiative (SCCVI), which provides



vulnerability assessment capability, and the Secure Configuration Remediation Initiative (SCRI) that provides vulnerability remediation capability. Below is an overview of the SCCVI and SCRI initiatives and the capabilities of each tool.

### **Secure Configuration Compliance Validation Initiative (SCCVI)**

SCCVI is comprised of eEye Digital Security's Retina Network Security Scanner and its *Remote Enterprise Management* (REM) console. The SCCVI tool is instrumental in downloading *Information Assurance Vulnerability Management* (IAVM) information, conducting scans to identify network assets impacted by the vulnerability, passing information to the Secure Configuration Remediation Initiative (SCRI) tool regarding impacted network assets, conducting vulnerability mitigation scans, and reporting IAVM compliance status to the DOD Information Assurance *Vulnerability Management System* (VMS) database.

The scanner can conduct two types of scans. For systems supported by the capability and for which it has administrative permissions, the SCCVI tool conducts an internal scan of the system's configuration and registry files. SCCVI supports most hardware systems, all operating systems and the majority of common software applications. For systems that the tool has not been provided administrative rights or the occasional software application not supported by SCCVI, the scanner will conduct an external 'ping' scan of the system. By scanning, SCCVI discovers assets and identifies known security vulnerabilities on various network platforms and technologies including servers, databases, switches, routers, and wireless access points.

The Remote Enterprise Manager (REM) allows multiple scanners to be managed from one centralized location. It also provides the ability for scanners to report their findings to one centralized location. Reports can be generated based on data collected from all of the scanners reporting to the REM.

## **Secure Configuration Remediation Initiative (SCRI)**

SCRI is comprised of Citadel Hercules technology. The SCRI tool imports information from the SCCVI tool (scanners) regarding impacted network assets and conducts remediation operations (i.e. software patch installations) to address the vulnerabilities.

Vulnerability remediation involves implementation of corrective actions to eliminate or mitigate identified vulnerabilities. Remediation actions may include implementation of a new or revised policy such as a firewall configuration change, frequent password change, type/character/length of password, as well as the installation of "patch" code to address vulnerability via software changes. Patch installation can be a time consuming, knowledge-intensive task and the use of automated methods to conduct patch installations greatly reduces the level of effort required to correct a given vulnerability.

The SCRI tool leverages the scanned data provided by SCCVI to apply patches, upgrades, fixes, or custom changes to a specific system or group of systems impacted by IAVM information to facilitate the automatic vulnerability remediation of devices on a network. The SCRI tool provides a sequence of automatically executable remediation steps known as 'remedies' that will correct each recognized vulnerability. Users of the product will download new patches from the government assigned website. The SCRI tool provides System Administrators with the ability to manage a large-scale vulnerability remediation process in a manner that is both systematic and comprehensive.

The principle components of the SCRI suite include the SCRI server, file download server, SCRI administrator, and SCRI clients. In addition to SCRI components, the system requires the Window 2000 Operating System and Microsoft IIS Web Server for reporting via remote server access.

## ***Hypothesis***

Vulnerability identification, remediation and compliance verification within DOD are currently inconsistent and non-integrated. The Secure Configuration Tool Suite solution should make significant grounds in resolving the Department of Defense deficiency with an Enterprise-Wide Information Assurance Vulnerability Management System.

## ***Purpose of Research***

The purpose of this document is to provide a plan for seamless deployment and integration of the SCTS tools by my employer into an organization's architecture. The deployment process is intended for installation of the tools whether they are implemented individually or as a package. The deployment process is intended to be a framework that can be modified as necessary for the specifics of a particular site.

The site selected is a major Combatant Command that is leading the way for the development of the proof of concept and eventually providing the baseline for concepts of operations as it relates to SCTS for all DOD to follow.

The project has five deployment phases: Initiation, Site Survey, Installation, Post-Installation and Sustainment. For each phase, entry and exit criteria were established. A description of each step is provided in Chapter Three.

Once the suite is installed the command which received the installation will provide the necessary feedback to make improvements of use and sustainment of these tools.

Specifically, the objectives of this feedback are:

- To provide an operational approach for the employment of SCCVI to facilitate asset identification, vulnerability assessment, and compliance reporting,

- To provide an operational approach for the employment of SCRI tools to expedite patch installation that addresses a software vulnerability,
- To provide an approach to obtain applicable service component and centrally managed program assets' vulnerability compliance status,
- To describe aspects of employment, training, and life cycle management associated with Secure Configuration Tool Suite employment in support of Information Assurance Vulnerability Management (IAVM) Program objectives.

### ***Limitations / Scope***

This project had a few limitations these limitations are as follows:

- Product selection for the initiatives were done prior to project being develop
- Security restrictions limit the amount of information that may be published in this paper
- The scope of the project was to evaluate the deployment process and not evaluate the products
- Unable to verify the software methodology process for development

### ***Definition of Terms***

Please see appendix D for a list of acronyms and the glossary for definition of terms at the end of this document.

### ***Summary***

This chapter provides the background information necessary to understand the importance of the project and its purpose. An overview is given of the two initiatives contained in the Secure Configuration Tool Suite (SCTS) and what tools were utilized. A hypothesis is stated and a description of the projects limitation is also provided.

## Chapter Two

### ***Overview***

Significant research was conducted prior to beginning this project. For the most part, the vendors provided most of the documentation needed for the technical side of the project. In addition, there were several DOD documents that were utilized as tasking orders provided by higher authority and used as guidelines for the installation. These documents are not available for public review, but the vendor's installation manuals, users manual, and operation manual have been identified in this document. If one has access to a .mil network, they will be able to review all the governing documents that were used in support of this project.

In an effort to broaden the author's mind to other possible solutions the DOD might have used, research was conducted on the Internet to evaluate other products. The evaluation was done based on the research material reviewed and not on actual hands on approach.

### ***Literature Review***

As for DOD's product selection for this project, curiosity struck the author as to whether there were better products out there that might have been utilized. From the vulnerability scanning perspective there are many to choose from. This author, on three other products, conducted a literary review in an effort to see if there were better products that DOD could have chosen from.

The three products chosen for the author's review where ISS, NetRecon, and Nessus.

- ISS Internet Scanner is an application-level vulnerability assessment that started off in '92 as a tiny Open Source scanner by Christopher Klaus. Now ISS has grown into a billion-dollar company. ISS Internet Scanner is pretty good, but is not cheap.

- Symantec NetRecon helps secure an organization's networks by exposing vulnerabilities before intruders can exploit and attack them. By automatically scanning systems and services on the network and safely simulating common intrusion or attack scenarios.
- Nessus, formerly an open source vulnerability assessment tool, is a remote security scanner for Linux, BSD, Solaris, and other Unices. It is plug-in-based, has a GTK interface, and performs over 1200 remote security checks. It allows for reports to be generated in HTML, XML, LaTeX, and ASCII text, and suggests solutions for security problems. It turned proprietary in late 2005

A March 2003 Information Security magazine review of five vulnerability assessment tools (including the ones I reviewed) was conducted and their final evaluation was similar to mind. Without micro-analyzing each product, which would be outside of the realm of this project, I believe it is safe to quote Mr. Snyder as saying, "None of the products we looked at excelled in all areas. Almost any might be good for a once-a-year scan of your network. But as day-to-day tools in the real world of corporate security, each had significant weaknesses." (Snyder) Snyder personally did not find one better than the other, the only issue he mentioned that supported the selection of Retina by DOD was that eEye Digital Security's Retina is a newer product that is still maturing, but it is one of the most promising of the products he reviewed.

It is for this reason that this author believes DOD chose Retina over all others. Of course, cost probably had a lot to do with it, but their flexibility to meet DOD needs and make the necessary addition could have been the primary reason for the product selection.

In addition, when you add the REM Security Management Platform, it enables network security managers to:

- Create an inventory of all assets

- Audit the assets and evaluate results of the audit
- Delegate tasks and, if necessary, remediate against vulnerabilities
- Generate Reports
- Perform a risk analysis

“With the REM Security Management Platform, network security personnel are able to plan, audit, assign tasks, remediate, and generate reports from a centralized location.” (eEye REM Operation Guide 1)

Most organizations this author worked for have some form of scanning devices or software for their network. They have some process in place to scan for known network vulnerabilities automatically. However, that is where the automation ends. Once vulnerability is discovered it is normally turned over to the security manager so he/she may prioritize the vulnerabilities for the security administrators. This is normally done to provide some form of protection against installing possible patches that may bring down the network, but it also means your network is vulnerable to the threats discovered until the network is patched.

In an interview that this author read on the Internet by IT Business Edge's Security Strategies section, they spoke with Dave Ostrowski, Product Marketing Manager, for Internet Security Systems Inc. (ISS) in Atlanta, and Scott Johnson, the company's product manager. In this interview Mr. Johnson put it best when it pertains to automated remediation when he said, “Not every customer wants to apply automatic updates, because frankly they're scared. If you just automatically apply something and it goes wrong, you've just applied that to your whole network.” (Schwartz) I believe this holds true anywhere you go.

However there are a growing number of products out there that claim to do automated remediation in some form or shape. For example,

Secure Elements Inc announced that its CLASS 5 Automated Vulnerability Remediation (AVR) product is a complete vulnerability management solution that enables IT security departments to proactively stop attacks before they start. The solution centralizes all aspects of vulnerability management, enabling users to automatically protect assets from most types of exploits, and to quickly locate, lock down and protect assets that have known vulnerabilities or that has rogue processes, unauthorized applications or invalid users on board. The CLASS 5 AVR standard modules include asset inventory and control, policy and audit management, active compliance and enforcement and vulnerability assessment and remediation. (Thomas)

Microsoft also has their version of patch management, which is known as Software Update Services, (SUS), or what is going to be used WSUS after 2006. This product “provides dynamic notification of critical updates to Windows computers as well as automatic distribution of those updates to your corporate Windows desktops and servers. For Software Update Services to function, only one corporate intranet computer requires access to the public Internet.”

(Microsoft)

Finally, the last product this author reviewed is called, Altiris. The reason this author reviewed this product was because the agency this author currently works for actually deployed the product on their own network. Altiris provided everything that Hercules does.

- Asset Monitoring
- Client & Mobile
- Security & Compliance
- Server & Infrastructure



Unfortunately even though the product claims to work on a UNIX environment, most of the UNIX administrators at my organization state that it does not work very well, mainly because Altirus states, "There may not be proper execution of our installation scripts in the cases where shell aliases are used." Most of the tactical machines used in a DOD environment are configured this way. While there is a work around, it is a tedious process, especially when one is dealing with a large quantity of UNIX boxes of different flavors.

For this initiative the Hercules product was selected. "The key features of the Hercules system include its interoperability with industry scanners and assessment tools, and a fully automated Remediation and Policy Enforcement solution. The remedy catalog of over 19,000 tested and proven remedies enables you to enforce security policies. The Hercules software is the only solution that enables remediation of all five classes of vulnerabilities: Unsecured Accounts, Unnecessary Services, Backdoors, Mis-configurations, and Software Defects." (Hercules User Manual)

### ***What is Known/Unknown about the Project***

The following information is known about the project:

- The Department of Defense has mandated the use of these tools
- The Combatant Command has been identified
- The product selected has been tested and verified to work as advertise
- Hardware has already been identified
- The baseline image for each product has been developed and tested

The following information is unknown about the project:

- What methodology was utilized for software development since these are commercial off the shelf products

- Government process for selecting the products that were utilized for this project. The author was not privy to this information

### ***Contribution the Project will make to the Field***

It is the author's opinion that this project will contribute considerably to the development, planning, and implementation process of any system being installed in a Department of Defense environment. The steps used in this project, i.e. phases, and all the documentation produced will contribute significantly to any other project that might develop at the author's present location.

## **Chapter Three**

### ***Methodology***

In the opinion of the author, the methodology used in this project for software development was the *Software Engineering Institute's Capability Maturity Model* (SEI CMM). Unfortunately, the author was unable to verify this with the vendor. Anyone that has ever researched the SEI CMM process knows that the tool was originally developed for the purpose of government contractors to perform contracted software projects. While the SEI CMM has five levels of maturity it is the author's opinion that the three products utilized in the two initiatives that comprise SCTS, are at a level three. Those standards that are needed to complete level two in the process have been established and the process for fine-tuning these standards is still on going. The five maturity levels of SEI CMM are as follows:

1. Initial
2. Repeatable
3. Defined
4. Managed

## 5. Optimizing

While this methodology focuses on software development, the *System Development Life Cycle* (SDLC) was modified to accommodate the Department of Defense's way of doing business. The project was comprised of five phases: Initiation, Site Survey, Installation, Post-Installation, and Sustainment. The table below illustrates the comparison with the SDLC.

| SDLC Comparison                                  |                                |
|--|--------------------------------|
| Project  | SDLC                           |
| Phase 1 Initiation                               | Planning Phase                 |
| Phase 2 Site Survey                              | Analysis Phase<br>Design Phase |
| Phase 3 Installation                             | Implementation Phase           |
| Phase 4 Post Installation<br>Phase 5 Sustainment | Support Phase                  |

**Table 1 SDLC Comparison with Project Phases**

### ***Specific Procedures***

The methodology selected worked according to plan. Specifically, for each phase, entry and exit criteria were established. These criteria's are discussed in the next chapter.

### **Initiation Phase**

The Initiation phase consisted of the initial contact with the site representatives, delivery of the implementation package, a pre-coordination meeting to walk through the Coordination Package, and the site submission of the completed site survey form. During this phase, each site provided sufficient information to make decisions regarding the use of the SCTS tools.

### **Site Survey Phase**

The Site Survey phase consisted of the Site Survey meeting, hardware configuration, and delivery and training. The purpose of this phase was to address technical aspects of the implementation, facility readiness, the technical solution, and the schedule.

## **Installation Phase**

The installation phase consisted of the Kick-Off meeting, installation of hardware and software, confirmation of the configuration, system familiarization, and the Out-Brief.

## **Post-Installation Phase**

The Post-Installation phase consisted of final coordination of the *Memorandum of Agreement* (MOA), documentation of the lessons learned, the start of the customer feedback cycle, and initiation of life-cycle support.

## **Sustainment Phase**

The Sustainment phase consisted of life-cycle support and feedback. Since this was the final phase there really were no exit criteria. It is an ongoing phase until the end of the life cycle of the product, which has not been determined.

## ***Deliverables***

The deliverables for this project was as follows:

- Provide hardware and software necessary for the installation of the suite in accordance with the *System Security Authorization Agreement* (SSAA).
- Install a fully functional SCTS and test that functionally based on MOA.
- Provide over the shoulder training to qualified administrators on site.

## ***Resource Requirements***

The following resources were required for the project:

- Installation Team
- Hardware
- Software plus Licenses
- Administrative Documentation.

- Network Connectivity
- The following ports need to be open based on product requirements
  - ✓ Retina - For scanning Windows boxes UDP ports 135, 137 and TCP ports 139 and 445 need to be open. For scanning a UNIX system, TCP port 22 should be open.
  - ✓ REM – Outbound TCP Port 21690 for Retina to REM communication and TCP Port 21692 for REM-to-REM communications.
  - ✓ Hercules – Outbound TCP port 80 for communications with the download server. Hercules also needs UDP ports 135 and 137 open as well as TCP 139 and 445 to remediate Windows boxes and TCP port 22 open to > remediate UNIX systems.
- Trained System Administrator that has administrator rights on local network prior to installation.

## **Outcome**

While there were hiccups during the installation, all phases were completed as planned. All of the findings were documented in the next chapter. The methodology used was perfect for this project. A lot was learned that lent to future installations.

## **Summary**

This chapter's main focus was to provide the background of the research method used in support of the project. It also provided a very brief comparison of the phases used in the project and how those relate to the System Development Life Cycle. The specific procedure required to proceed with the project was introduced and deliverables and resource requirements were identified. Finally, the outcome of the project was stated.

## Chapter 4

### ***Project History***

This project started late September of 2005 and pretty much was completed late November 2005. Each phase was executed according to plan and all exit criteria met with the exceptions of those noted in this paper. Team members were assigned their install locations during Phase Two of the project. Upon conclusion of the project all that was desired was obtained.

### **How the project was managed**

As stated before the project was managed by strict adherence to the phases developed for execution. Below are tables which define the entry and exit criteria of each phase.

Phase One:

| <b><i>Entry Criteria</i></b>                | <b><i>Exit Criteria</i></b>                |
|---|--|
| Signed ATO                                  | Established Communication with On-site Rep |
| Tool Release Announcement to the Enterprise | Established Communication with Site POC    |
| Up-to-date Coordination Package             | Completed Coordination Meeting             |
|   | Completed Site Survey Form                 |
|   | Scheduled Site Survey Meeting              |

**Table 2 Initiation Phase: Entry and Exit Criteria**

Phase Two:

| <b><i>Entry Criteria</i></b>               | <b><i>Exit Criteria</i></b>                  |
|--|--|
| Established Communication with On-site Rep | Trained Staff                                |
| Established Communication with Site POC    | Defined Technical Solution                   |
| Completed Coordination Meeting             | Coordinated Installation Schedule Milestones |
| Completed Site Survey Form                 | Closed Critical Action Items                 |
| Scheduled Site Survey Meeting              | In-Processed Hardware at Site                |

**Table 3 Site Survey Phase: Entry and Exit Criteria**

Phase Three:

| <b><i>Entry Criteria</i></b>                 | <b><i>Exit Criteria</i></b>     |
|--|---------------------------------|
| Trained Staff                                | Installed Technical Solution    |
| Defined Technical Solution                   | Completed Familiarization       |
| Coordinated Installation Schedule Milestones | Signed Property Transfer (1149) |
| Closed Critical Action Items                 | Completed Out-Brief             |
| In-processed Hardware                        | Documented Status               |

**Table 4 Installation Phase: Entry and Exit Criteria**

Phase Four:

| <i>Entry Criteria</i>        | <i>Exit Criteria</i>              |
|------------------------------|-----------------------------------|
| Installed Technical Solution | Initiated Life-Cycle Support      |
| Completed Familiarization    | Quality Controlled                |
| Signed Property Transfer     | Documented Lessons Learned        |
| Completed Out-Brief          | Finalized Memorandum of Agreement |
| Documented Status            |                                   |

**Table 5 Post Installation Phase: Entry and Exit Criteria**

Phase Five:

| <i>Entry Criteria</i>             | <i>Exit Criteria</i> |
|-----------------------------------|----------------------|
| Initiated Life Cycle Support      |                      |
| Quality Controlled                |                      |
| Documented Lessons Learned        |                      |
| Finalized Memorandum of Agreement |                      |

**Table 6 Sustainment Phase: Entry and Exit Criteria**

**Changes to project**

As the tools were installed at the sub-component sites there was a transition into what would be defined as the implantation, which was when the site began to utilize the tools and started to implement the processes which should have eventually ended up with the report of their asset status being relayed up to the REM Server at the Combatant Command. Unfortunately, this did not happen for the reasons mentioned above.

These processes should have consisted of a completed Retina scan with at a minimum the DOD IAVA policy, against 100% of each site’s assets, followed by a remediation to the extent that the operational sub-component would have allowed. Once the remediation was completed, there should have been a 100% rescan of the network using the same policy and the results would have then been reported up to the REM Server at the Combatant Command. This, of course, did not happen either. However, if all the sub-components completed their respected network scans and reported this to the Combatant Command’s REM Server, this would have ultimately given a complete picture of the security posture of that Combatant Command and its sub-components.

This was anticipated during this installation. Appendix C shows a simulation of how the SCTS was installed at this Combatant Command and its sub-components.

### **Where goals meet**

The Secure Configuration Tool Suite solution will make significant gains in resolving the DOD's deficiency with an Enterprise-wide Information Assurance Vulnerability Management System, the products proved themselves in the field during this project and the baseline implementation plan was effective.

The two goals established for this project were reached,

1. Develop a plan for seamless deployment and integration to be used as the baseline for future installations at other DoD components
2. Develop a concept of operation for reporting within these components

However, a consensus needs to be established for the concept of operations on reporting.

### **Findings**

It was evident to this author that a better job could have been performed in preparation of this installation. While all steps were taken to follow each phase prior to proceeding to the next, a lot of issues were taken for granted. Some of the technical issues discovered during the installation were as follows:

- Ports 21690 and 21692 were not open prior to arriving costing a delay of four hours
- Access to the DOD designated download server for Hercules was not permitted from within the command
- Site Responsibility agreements prior to installation team arrival were not adhered to, thus delaying software installation



- None of the System Administrators remembered prior training
- Command would not allow my company's baseline scanner on their network
- Command did not trust automated remediation
- One sub-component command had received a damaged server, unable to install Hercules
- One sub-component did not even know we were coming and canceled the installation until Phase 1 and 2 were complete at their site
- Numerous firewall issues amongst the combatant command and its subcomponents. Lack of communication hindered the installation

Unfortunately it was not the technical issues that presented the biggest challenges in this project. The biggest challenges presented were the bureaucratic red tape that were addressed and ignored. Whether a military installation or a commercial business, change is a hard thing to accept. This project introduced changes in reporting network vulnerability status which created an atmosphere of fear on who would see what. In addition the idea to automate the remediation process was not accepted very well, most of the administrators were reluctant to allow an automated product to do the patching of vulnerabilities on workstations, but most importantly on their servers themselves.

### ***Summary of Results***

The Combatant Command that was selected had a very complex network, making it difficult to work with both local and sub-component networks. Firewalls/routers were supposed to be open to sub-component sites prior to the arrival of the installation teams, however they were not. Sub-components sent the necessary waiver forms, requesting the Combatant Command's firewalls to be opened for their scanners, but the forms had to be resubmitted multiple times due to errors

such as incorrect ports and IP's. In addition, it did not help that Firewalls were going thru scheduled maintenance, so they were up and down throughout this installation.

All this could have been avoided had the Combatant Command followed through with all agreements made during the first three phases of this project.

It was evident to this author that all key players needed to be involved throughout the whole process and not just entering the picture during Phase Three. The resistance to change and all the technical issues that surfaced could have been avoided if everyone was involved from the beginning.

From an installer's point of view the project installation was a success. All suites were installed at their respected site and within each site everything worked as advertised. Unfortunately, the internal operational objectives or commitments set the project up for failure and the initial goal of providing an Enterprise reporting and remediation tool was not achieved at the enterprise level. At the local level administrators tested the products and while there was a reluctance to commit to the product it was evident to this author that there was overwhelming interest to utilize the product once the product gained their trust.

A lot was learned from this project and have since been applied on subsequent installations.

While the Combatant Command is still working out their reporting policy with each of the sub-components, the sub-components are using the products at their respected site. Feedback received on issues that are relevant and benefit all have been applied based on these feedback reports.

## Chapter 5

### ***What was learned***

So much was learned during this project. To try to document everything in the author's opinion is impossible. However, below is a breakdown of issues that were encountered during the process. It has been broken into two categories: Technical and Non-Technical. One must keep in mind that some of the technical issues are specific to DOD configuration of any system and may not apply to a commercial entity.

#### **Technical:**

- The Rename Script provided by my employer does not need to be run when changing the Hercules Server IP address, only when changing the NETBIOS name.
- Hercules will not remediate GLOBAL POLICY in an Active Directory network. It will change LOCAL POLICY on a system, but this will not affect the entire domain.
- Place the Hercules Server outside the domain if possible. This eliminates any possible DOMAIN SECURITY POLICY problems such as removing user permissions from the Hercules box.
- Hercules client names should be less than fifteen characters.
- When scanning an active directory network it was determined that if certain options were enabled within the scanner, Retina will lockout accounts. The settings have been narrowed down to: *Enumerating Users via NetBIOS* and the three password checks. The only check that is enabled by default in the IAVA audit is the *Enumerating Users via NetBIOS* (under options). If one is scanning an active directory network you will want to turn these options off.

- Retina/REM Permission issues - IUSR accounts need the following permissions at a minimum in order for REM to function correctly:
  - REM Events Manager\ -- Modify
  - REM Events Manager\\*.xml -- Modify
  - REM Events Manager\\*.dll -- Read
  - REM Events Manager\HTML\ -- Read (recursive)
  - REM Events Manager\HTML\Reports -- Modify (recursive)
  - REM Events Manager\HTML\export -- Modify (recursive)
  - REM Events Manager\JobQueues\ -- Modify (recursive)
  - REM Events Manager\Templates -- Read (recursive)
  - Retina5\retinaconfig.xml -- Read + Write
  - Retina5\Groups -- Modify (recursive)
  - Retina 5\Scans\Jobs\REM -- Read + Write (recursive)

### **Non-Technical:**

- Bring our own rack hardware toolkit (ex. Screwdriver, etc.).
- Ensure everyone is involved in the process starting from Phase 1.
- Contact actual administrators to get a realistic confirmation of the site survey and validate its content.
- Ensure a government representative from this author's agency is present or available on request.

### **What would have been done differently**

From the author's perspective the biggest thing that would be done differently for this project occurs in Phase Four, finalizing the Memorandum of Agreement. It is the author's belief that

much of the political rhetoric described in this paper could have been resolved if this document was finalized during Phase Two and established as an exit criteria for that phase.

### ***Possible Future Work***

The SCTS is gaining momentum since the end of this installation. A new version has hit the street and testing has been completed. All future installations will be based on a 2003 platform with XP scanners. Everything learned from this installation have been incorporated into future installs in an effort not to repeat the same mistakes.

The initial problems presented during this project have long since been forgotten. The team and the author continue to march forward with more installations throughout DOD. The new tasking order that mandated the item be implemented by 2008 has done a lot for eliminating the political rhetoric that we had to endure.

We are receiving more requests for the installations of these products daily. Since the end of this project, this author has personally installed ten suites at ten different locations on my own, which is not to mention what the other nine members of the team have done.

Customers are starting to learn the value of what the Secure Configuration Tool Suite has to offer to their network as it relates to Information Assurance, bringing DOD one step closer to the ultimate IA tool suite.

### ***Conclusions / recommendations***

A lot of preparation and man-hours were dedicated to the completion of this project. It is this author's opinion that the Secure Configuration Tool Suite solution will make significant grounds in resolving the DOD's deficiency with an Enterprise-wide Information Assurance Vulnerability Management System.

These products proved themselves in the field and while everything did not go exactly according to plans, the project, in this author's opinion, was a success. As a former Information System's Officer in the United States Navy, this author would have done back flips if these products were available. The ability to scan a network for compliancy and then remediate your deficiencies at a click of a button is worth the changes one has to make in their environment.

As more systems are deployed so does the interest in the products and the initiative. This author looks forward to seeing this initiative go full circle.

### ***Summary***

For the last few years the Department of Defense has been advertising the Secure Configuration Tool Suite as the tool that will assist in the resolution of vulnerability identification, remediation, and compliance verification in a consistent and integrated manner within the Department of Defense.

The project documented in this paper was an effort to develop a baseline for deployment to be utilized in future installations. In addition, a proof of concept on reporting these vulnerabilities and compliancy was also being developed. The project succeeded in both efforts in the opinion of the author; although, some may interpret some of the writings in this paper to indicate otherwise.

This paper should be useful as a guideline for installing the two products anywhere. The network diagram in Appendix C should give anyone an idea how these three systems interface. The site surveys can be tailored to anyone's needs.

The whole process, to include writing and briefing this paper has resulted in such a wealth of knowledge that is impossible to measure. The author sincerely hopes that the readers of this document will benefit as well.

# Appendix A – SCCVI Site Survey checklist

## *SCCVI Site Survey*

**Site Location** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Dates On-Site:** \_\_\_\_\_

**Assigned Tech(s)** \_\_\_\_\_

**Security Clearance POC:** \_\_\_\_\_  
**Phone Number:** \_\_\_\_\_  
**Fax Number:** \_\_\_\_\_  
**E-mail address:** \_\_\_\_\_  
\_\_\_\_\_

**Security Clearance(s) Sent:**  Yes  No

**POC Name:** \_\_\_\_\_  
**Phone Number** \_\_\_\_\_  
**Email Address:** \_\_\_\_\_

**Networking Personnel:** \_\_\_\_\_  
**Phone Number** \_\_\_\_\_  
**Email Address:** \_\_\_\_\_

**Operations Personnel:** \_\_\_\_\_  
**Phone Number** \_\_\_\_\_  
**Email Address:** \_\_\_\_\_

**REM:** \_\_\_\_\_  
**System Name** \_\_\_\_\_  
**(NetBIOS):** \_\_\_\_\_  
**System IP:** \_\_\_\_\_

|  |
|--|
|  |
|--|

**MOA:** \_\_\_\_\_

**SSAA:** \_\_\_\_\_

|  |
|--|
|  |
|--|

|  |            |           |
|--|------------|-----------|
| <b>Can XXX get an approved server name and IP address before install? (if yes list information in System Configuration Information area on page 1)</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|  |            |           |
|--|------------|-----------|
| <b>Can you get a copy of a network diagram and any network information beforehand?</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Base Network Topology Diagrams – IP address space included</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Will SCCVI equipment be interfaced with a proxy?</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Does the network administrator have access to modify the Firewall?</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|

|  |            |           |
|--|------------|-----------|
| <b>Ports: 21690, 21692, 80 or 443 have been opened for SCCVI operation</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>What is the CCB process to get equipment on network (list on last sheet)</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|

|  |            |           |
|--|------------|-----------|
| <b>Does local policy allow for server service to be running?</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|  |            |           |
|--|------------|-----------|
| <b>Is Server Service currently running on all network systems? (Needed for Retina)</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|  |            |           |
|--|------------|-----------|
| <b>Does local policy allow for remote registry access? (Needed for Retina)</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|  |            |           |
|--|------------|-----------|
| <b>Is remote registry access currently enabled on all network systems?</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Will the Windows devices have the three default administration shares (C\$, IPC\$, ADMIN\$) turned on?</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|



|  |            |           |
|--|------------|-----------|
| <b>Bandwidth limitations if any (3KB – 11 KB needed)</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Do we have approval to connect to the network?</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>What is the network speed (10/100, Gig)?</b> | <b>Yes</b> | <b>No</b> |
|---|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Rack requirements is 1U for REM; Retina is a laptop</b>                  |            |           |
| <b>Is space available?</b>  | <b>Yes</b> | <b>No</b> |
| <b>Square or round holes for mounting?</b>                                  | <b>S</b>   | <b>R</b>  |
| <b>Width and depth of racks? Need specs</b>                                 |            |           |
| <b>Are shelves available if racks are incompatible</b>                      |            |           |
| <b>Power requirements met</b>   |            |           |
| <i>Note: Systems will not be deployed with a monitor, keyboard or mouse</i> |            |           |

|                                  |            |           |
|----------------------------------|------------|-----------|
| <b>DAA to approve connection</b> | <b>Yes</b> | <b>No</b> |
|----------------------------------|------------|-----------|

|   |  |
|---|--|
| <b>Who needs to be notified for approval to install new software and hardware onto the network?</b> |  |
|---|--|

|  |            |           |
|--|------------|-----------|
| <b>Are the SA's certified through DISA (either on-line or classroom) for REM/Retina?</b> | <b>Yes</b> | <b>No</b> |
|--|------------|-----------|

|   |            |           |
|---|------------|-----------|
| <b>Are there are "work time constraints" – e.g. No overtime allowed, XXX team must report to work at certain time, or leave by certain time, etc? If so, list below. This could impact number of days XXX team needs to complete install.</b> | <b>Yes</b> | <b>No</b> |
|   |            |           |
|   |            |           |
|   |            |           |

**PBO Name (Site):** \_\_\_\_\_

**PBO Telephone Number:** \_\_\_\_\_

**PBO e-mail Address:** \_\_\_\_\_

**Site Mailing Address:** \_\_\_\_\_

\_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

**Mark For (POC name):** \_\_\_\_\_

**POC Telephone Number:** \_\_\_\_\_

**Completed Shipping Checklist:**  **Yes**  **No**

**Date Shipped:** \_\_\_\_\_

**Date of Clone used:**  
(to verify IAVAs/Patches/AV dates) \_\_\_\_\_

**FedEx Tracking Number (s)** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

# Appendix B – SCRI Site Survey checklist

## *SCRI Site Survey*



**Site Location** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Dates On-Site:** \_\_\_\_\_

**Assigned Tech(s)** \_\_\_\_\_

**Security Clearance POC:** \_\_\_\_\_

**Phone Number:** \_\_\_\_\_

**Fax Number:** \_\_\_\_\_

**E-mail address:** \_\_\_\_\_

**Security Clearance(s) Sent:**  Yes  No



**POC Name:** \_\_\_\_\_

**Phone Number** \_\_\_\_\_

**Email Address:** \_\_\_\_\_

**Backup POC Name:** \_\_\_\_\_

**Phone Number** \_\_\_\_\_

**Email Address:** \_\_\_\_\_

**Networking Personnel:** \_\_\_\_\_

**Phone Number** \_\_\_\_\_

**Email Address:** \_\_\_\_\_

**Operations Personnel:** \_\_\_\_\_

**Phone Number** \_\_\_\_\_

**Email Address:** \_\_\_\_\_

\_\_\_\_\_

MOA: \_\_\_\_\_

SSAA:

Can XXX get a copy of a network diagram and any network information beforehand?

Can XXX get an approved server name and IP address before install? (if yes list information on last sheet)

Does the network administrator have access to modify the Firewall and or local routers?

What is the CCB process to get equipment on network (list on last sheet)?

Does local policy allow for agents to be used on systems?

Does local policy allow for server service to be running?

Is Server Service currently running on all Windows network systems?

Does local policy allow for remote registry access?

Is remote registry access currently enabled on all network systems?

Can site supply a workstation for Hercules Admin console to be installed on? (this is the management software for the Hercules server – see specs below)

Will your Unix clients have SSH 3.5p1 or greater installed?

Are there HTTP, HTTPS or FTP proxies between the Hercules server and the Download server in Montgomery?

Will Hercules be able to utilize Windows administrator accounts that have access to remote Windows devices that remote installation of the Hercules client is required?

Will the Windows devices have the three default administration shares (C\$, IPC\$, ADMIN\$) turned on?

|   |                  |
|---|------------------|
| <b>Will the Windows devices allow remote registry access?</b>   |                  |
| <b>Will Hercules be allowed to create a Windows domain administration account for remote installation and administration of the Hercules client?</b>  |                  |
| <b>Are all the sites under a single domain?</b>   |                  |
| <b>Have you reviewed the Windows client device minimum requirements and do yours meet them?</b>   |                  |
| <b>Have you reviewed the Unix client device minimum requirements and do yours meet them?</b>  |                  |
| <b>Is the SSH TCP/IP port 22 enabled in your network to allow remote installation and administration of the Unix Hercules client?</b>   |                  |
| <b>Are there Windows desktop firewalls in place and if so, will it prohibit outbound HTTP/HTTPS access by the Hercules clients?</b>   |                  |
| <b>Bandwidth limitations, if any? (explain below)</b>   |                  |
| <b>Will site be able to obtain a SSL Certificate (if needed) from DOD for Hercules server?</b>  |                  |
| <b>Do we have approval to connect to the network?</b>   |                  |
| <b>What is the network speed (10/100, Gig)?</b>   |                  |
| <b>Rack requirements (Hercules server is 2U – Combo REM/Hercules is 3U)</b>   |                  |
| <b>Is space available?</b>  |                  |
| <b>Square or round holes for mounting?</b>  |                  |
| <b>Width and depth of racks? Need specs</b>   |                  |
| <b>Are shelves available if racks are incompatible</b>  |                  |
| <b>Power requirements met? (dual power supplies)</b>  |                  |
| <b>DAA to approve connection?</b>   |                  |
| <b>Who needs to be notified for approval to install new software and hardware onto the network?</b>   |                  |
| <b>Are there are “work time constraints” – e.g. No overtime allowed, XXX team must report to work at certain time, or leave by certain time, etc? If so, list below. This could impact number of days XXX team needs to complete install.</b> | <b>Yes    No</b> |
|   |                  |
|   |                  |
|   |                  |

Please list the estimated amount of each type of OS that the client software will be installed on.

- Windows NT 4 Workstations \_\_\_\_\_
- Windows NT 4 Terminal Servers \_\_\_\_\_
- Windows NT 4 Server \_\_\_\_\_
- Windows 2000 \_\_\_\_\_
- Windows XP \_\_\_\_\_
- Windows 2003 \_\_\_\_\_
- Sun Solaris \_\_\_\_\_
- Red Hat Linux \_\_\_\_\_
- IBM AIX \_\_\_\_\_
- HP HP-UX \_\_\_\_\_
- Apple Mac OS X \_\_\_\_\_

The Hercules Server must meet the following requirements (if you installing your own):

| Operating Systems | Windows® 2000 Server, SP4<br>Windows® 2000 Advanced Server, SP4<br>Windows Server™ 2003 Standard Edition<br>Windows Server™ 2003 Enterprise Edition | <ul style="list-style-type: none"> <li>• The Hercules Server can be installed on top of an existing MSDE or SQL Server 2000 installation.</li> <li>• The Hercules Server cannot be installed on a machine that is either a Primary (PDC) or Backup Domain Controller (BDC) or Active Directory Controller (ADC).</li> <li>• SSL is used for secure communication.</li> <li>• Software, IIS and Web Browser must be installed prior to installing the Hercules Server.</li> </ul> |
|-------------------|---|--|
| Processor         | Pentium® 4, 2 GHz or above  |  |
| Memory            | 512 MB RAM or above   |  |
| Free Disk Space   | 2.8 GB for server installation<br>5.0 GB for server upgrade   |  |
| VGA Graphics      | 1024x768 resolution   |  |
| Network Interface | 100 Mb/s  |  |
| Web Browser       | Internet Explorer® 6.0 SP1  |  |
| Web Server        | IIS 5.0 (Windows® 2000 Server family)   |  |
| Software          | Microsoft®.NET Framework v1.1<br>Microsoft® <u>ASP.NET</u> for Windows Server 2003<br>Adobe Acrobat Reader™ 6.02 or higher                          |  |

The following are requirements for running the Hercules Administrator Console:

| Operating Systems | Windows 2000 Server, SP4<br>Windows 2000 Advanced Server, SP4<br>Windows® 2000 Professional, SP4<br>Windows® XP Professional, all SP<br>Windows Server 2003 Standard Edition<br>Windows Server 2003 Enterprise Edition | <ul style="list-style-type: none"> <li>• The Hercules Administrator can run on the same machine as the Hercules Server, but additional disk space and memory will be needed.</li> <li>• The user of the Hercules Administrator must be using either a valid local Microsoft Windows account on the Hercules Server or a domain account recognized by the Hercules Server.</li> </ul> |
|-------------------|--|--|
| Processor         | Pentium III, 750 MHz or above  |  |
| Memory            | 256 MB RAM or above  |  |
| Free Disk Space   | 1 GB or above  |  |
| VGA Graphics      | 1024x768 resolution  |  |
| Network Interface | 100 Mb/s   |  |
| Web Browser       | Internet Explorer 5.5 or above   |  |
| Software          | Microsoft .NET Framework v1.1<br>Adobe Acrobat Reader 6.02 or higher   |  |

## Hercules Windows Client Requirements:

| Operating Systems | Windows 2000 Server, all Service Packs (SP)<br>Windows 2000 Advanced Server, all SP<br>Windows 2000 Professional, all SP<br>Windows NT® 4.0 Workstation, SP6<br>Windows NT® 4.0 Standard Server, SP6<br>Windows NT® 4.0 Terminal Server, SP6<br>Windows XP Professional, all SP<br>Windows Server 2003 Standard Edition<br>Windows Server 2003 Enterprise Edition<br>Windows Server™ 2003 Small Business Edition<br>Windows Server™ 2003 Web Edition | <ul style="list-style-type: none"> <li>• Disk space for patch downloads depends on size of patches, service packs, and hot fixes.</li> <li>• For services that must be running prior to installation, see <i>Hercules User's Guide</i>.</li> </ul> |
|-------------------|--|--|
| Processor         | Pentium II or above  |  |
| Memory            | 64 MB RAM or above   |  |
| Free Disk Space   | 15 MB for client installation<br>5 GB for patch downloads  |  |
| Web Browser       | Internet Explorer 5.5 SP2 or above, only to support Windows NT 4.0 platforms   |  |
| Security          | SSL used for secure communications   |  |



## Hercules Solaris Client Requirements:

|                   |   |  |
|-------------------|---|--|
|                   |   |  |
| Operating Systems | Solaris™ 2.6, 7, 8, 9   | <ul style="list-style-type: none"> <li>Hercules Client operates at run level 3</li> </ul>  |
| Processor         | SPARC®  | <ul style="list-style-type: none"> <li>Outbound access via HTTP/HTTPS</li> </ul>   |
| Memory            | 64 MB RAM or above  | <ul style="list-style-type: none"> <li>(SSH) Inbound root access via TCP/IP port 22</li> </ul>   |
| Free Disk Space   | 15 MB in /opt for client install and msg logging<br>200 MB for patch download to /opt/citadel/hercules/download   | <ul style="list-style-type: none"> <li>Patch clusters recommended for downloads</li> <li>Disk space for patch download depends on size of patches and packages to download.</li> </ul> |
| Software          | (Solaris 2.6 only) gzip for 2.6_Recommended. tar. Z files   | <ul style="list-style-type: none"> <li>Install gzip and unzip in /bin or /usr/local/bin so client can unzip Solaris packages.</li> </ul>   |
| Security Software | <ul style="list-style-type: none"> <li>OpenSSH v3.5p1 or higher</li> <li>SSL/HTTPS enabled with OpenSSL 0.96 or higher</li> <li>(Solaris 8 only) requires patch 112438-01 to enable SSL and SSH</li> <li>Sudo v1.6.7 or later (optional)</li> </ul> | <ul style="list-style-type: none"> <li>Citadel recommends sudo access for enhanced security.</li> </ul>  |

a. If you are running Solaris 2.6, and want to remediate a vulnerability that requires the 2.6\_Recommended. tar.Zfile downloaded from sunsolve.sun.com and installed on the server, you must first have the gzip package installed. It does not come installed by default in this older version of Solaris. Solaris 7, 8, and 9 do not have this issue.

## Hercules Red Hat Client Requirements:

|                   |   |   |
|-------------------|---|---|
| Operating Systems | Red Hat 6.0, 6.1, 6.2, 7.0, 7.1, 7.2, 7.3, 8, 9   | <ul style="list-style-type: none"> <li>• Hercules Client operates at run level 3</li> <li>• Outbound access via HTTP/HTTPS</li> <li>• Disk space for patch downloads depends on size of RPMs to download.</li> </ul>    |
| Processor         | Pentium II class  |   |
| Memory            | 64 MB RAM or above  |   |
| Free Disk Space   | 15 MB in /opt for client install and msg logging<br>200 MB for patch downloads to /opt/citadel/hercules/download  |   |
| Software          | <p>Minimum RPM package versions required:</p> <ul style="list-style-type: none"> <li>• bzip2-0.9.5d-2.i386.rpm</li> <li>• db3-3.1<sup>a</sup></li> <li>• popt-1.5-9.6x.i386.rpm</li> <li>• rpm-4.0.2-6x.i386.rpm</li> </ul> | <ul style="list-style-type: none"> <li>• If these packages are not installed, you will need to install them (in the order listed).</li> <li>• Red Hat 7.3 should already include the bzip and popt packages.</li> </ul> |
| Security Software | <ul style="list-style-type: none"> <li>• OpenSSH v3.5p1 or higher</li> <li>• SSL/HTTPS enabled with OpenSSL 0.9.6 or higher</li> <li>• Sudo v1.6.7 or later (optional)</li> </ul>   | <ul style="list-style-type: none"> <li>• (SSH) Inbound root access via TCP/IP port 22</li> <li>• Citadel recommends sudo access for enhanced security. By default, sudo is installed with Red Hat v8 and v9.</li> </ul> |

a. For Red Hat 6.0 and 6.1, use db3~3.1.17~4.6xi.386.rpm instead. In Hercules 2.2.0, Citadel stopped providing new remedies for Red Hat Linux 6.0 and 6.1 because these versions are no longer supported by Red Hat.

## Hercules AIX Client Requirements:

| Platforms         | AIX 5.1, 5.2  | <ul style="list-style-type: none"> <li>• Hercules Client operates at run level 2</li> <li>• Outbound access via HTTP/HTTPS</li> <li>• Disk space for patch downloads depends on size of bff or .tar.gz files to download.</li> </ul> |
|-------------------|---|--|
| Processor         | PowerPC™  |  |
| Memory            | 128 MB RAM or above   |  |
| Free Disk Space   | 15 MB in /opt for client install<br>2 GB for patch downloads in /opt/citadel/hercules/download  |  |
| Security Software | <ul style="list-style-type: none"> <li>• OpenSSH v3.5p1 or higher</li> <li>• SSL/HTTPS enabled with OpenSSL 0.9.6 or higher</li> <li>• Sudo v1.6.7 or later (optional)</li> </ul> | <ul style="list-style-type: none"> <li>• (SSH) Inbound root access via TCP/IP port 22</li> <li>• Citadel recommends sudo access for enhanced security</li> </ul>   |

## Hercules HP-UX Client Requirements:

| Platforms         | HP-UX 11.0, 11 iv1  | <ul style="list-style-type: none"> <li>• Hercules Client operates at run level 3</li> <li>• Outbound access via HTTP/HTTPS</li> <li>• Disk space for patch downloads depends on size of the depot files to download.</li> </ul> |
|-------------------|---|---|
| Processor         | PA-RISC™  |   |
| Memory            | 128 MB RAM or above   |   |
| Free Disk Space   | 15 MB in /opt for client install<br>1 GB for patch download in /opt/citadel/hercules/download   |   |
| Software          | Requires the following or superseding patches:<br>PHSS_28869 (for HP-UX 11.0)<br>PHSS_28871 (for HP-UX 11 iv1)  | • "Download latest patches for HP-UX 11.0 and 11iv1"  |
| Security Software | <ul style="list-style-type: none"> <li>• OpenSSH v3.5p1 or higher</li> <li>• SSL/HTTPS enabled with OpenSSL 0.9.6 or higher</li> <li>• Sudo v1.6.7 or later (optional)</li> </ul> | <ul style="list-style-type: none"> <li>• (SSH) Inbound root access via TCP/IP port 22</li> <li>• Citadel recommends sudo access for enhanced security</li> </ul>  |

Hercules OS X Client Requirements:

| Platforms         | Mac OS X 10.2 (Jaguar)   | <ul style="list-style-type: none"> <li>• Hercules Client runs as a daemon</li> <li>• Outbound access via HTTP/HTTPS</li> <li>• Disk space for patch downloads depends on size of the disk image (dmg) files to download.</li> </ul> |
|-------------------|--|---|
| Processor         | PowerPC™   |   |
| Memory            | 128 MB RAM or above  |   |
| Free Disk Space   | 15 MB in /opt for client install<br>200 MB for patch download in /opt/citadel/hercules/download  |   |
| Security Software | <ul style="list-style-type: none"> <li>• OpenSSH v3.6.1 p1 or higher</li> <li>• SSL/HTTPS enabled with OpenSSL 0.9.6 or higher</li> <li>• Sudo v1.6.7 or later (optional)</li> </ul> | <ul style="list-style-type: none"> <li>• (SSH) Inbound root access via TCP/IP port 22.</li> <li>• Citadel recommends sudo access for enhanced security. By default, sudo is installed with the Mac OS X.</li> </ul>                 |

a. This version is different than that required for the other clients.



**PBO Name (Site):** \_\_\_\_\_

**PBO Telephone Number:** \_\_\_\_\_

**PBO e-mail Address:** \_\_\_\_\_

**Site Mailing Address:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Mark For (POC name):** \_\_\_\_\_

**POC Telephone Number:** \_\_\_\_\_

**Completed Shipping Checklist:**  **Yes**  **No**

**Date Shipped:** \_\_\_\_\_

**Date of Clone used:**  
\_\_\_\_\_

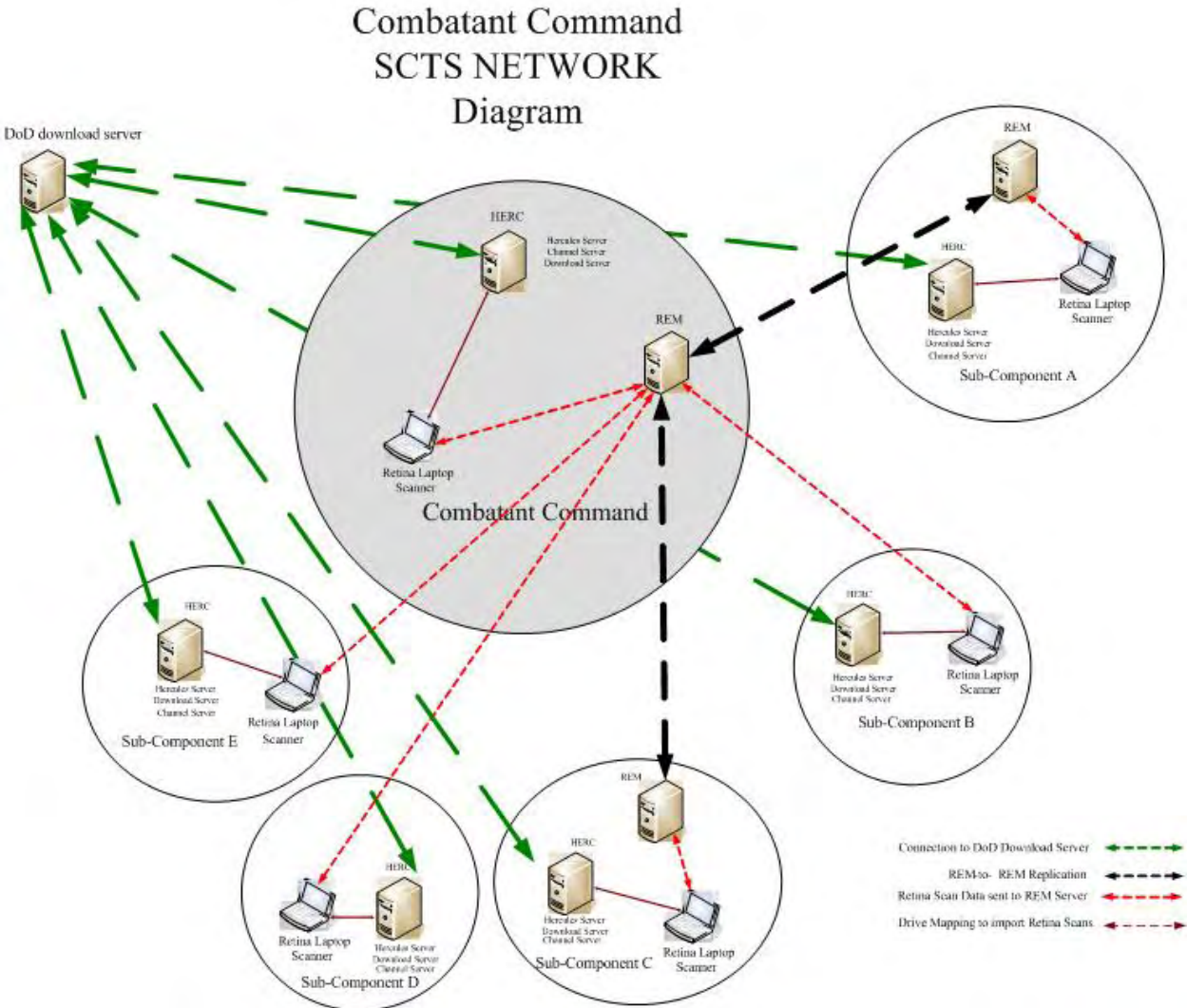
**FedEx Tracking Number (s)** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_



**Site-specific  
information and/or  
comments.**



# Appendix C – Network Diagram of Installation



**Figure 1 Network Diagram of Installation**

The network diagram above is not an actual site-specific drawing. This is just a representation of the design used due to security concerns of actually publishing a combatant command's network diagram on the Internet. The number of site represented in the diagram does not reflect the actual number of sites the SCTS was installed at for this project.

## **Appendix D – Acronym Listing**

ATO – Authority to Operate

AVR - Automated Vulnerability Remediation

CM - Configuration Management

CMM - Capability Maturity Model

CND – Computer Network Defense

COCOMS - Combatant Commands

CONOPS - Concept of Operations

DOD – Department of Defense

ESSG – Enterprise Solutions Steering Group

HTTP - HyperText Transfer Protocol

HTTPS - HyperText Transfer Protocol (Secure)

IA – Information Assurance

IAVM - Information Assurance Vulnerability Management

IDS - Intrusion Detection System

IIS – Internet Information Services

IP - Internet Protocol

IS - Information System

IT - Information Technology

LAN - Local Area Network

MOA - Memorandum of Agreement

MOU - Memorandum of Understanding

POC - Point of Contact



REM - Remote Enterprise Management

SA - System Administrator

SCCVI – Secure Configuration Compliance Validation Initiative

SCRI – Secure Configuration Remediation Initiative

SCTS - Secure Configuration Tool Suite

SEI - Software Engineering Institute

SMS - Systems Management Server

SSAA – System Security Authorization Agreement

TCP/IP - Transmission Control Protocol/Internet Protocol

VA – Vulnerability Assessment

VMS - Vulnerability Management System

## Glossary of Terms

*Accountability* - The property that allows the ability to identify, verifies, and traces system entities as well as changes in status. Accountability is considered to include authenticity and non-repudiation.

*Accreditation* - The formal declaration by an Accreditor that an AIS, site, application, or network is approved to operate in a particular security mode using a prescribed set of safeguards.

*Architecture* - The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment, and services, including support services and related resources.

*Assurance* - A measure of confidence that the security features and architecture of an AIS, site, application, or network accurately mediate and enforce security policies and is composed of the degree of availability, confidentiality, accountability, and integrity required of the AIS, site, application, or network.

*Configuration Control* - Process of controlling modifications to an IT system's hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

*Configuration Management (CM)* - Management of security features and assurances through control of changes made to hardware, firmware, software, documentation, test, test fixtures, and test documentation of an automated information system throughout the development and operational life of a system.

*Designated Approving Authority (DAA)* - Official with authority to formally assume responsibility for operating an AIS, site, application, or network at an acceptable level of risk.

*Developer* - The organization or individual that develops the information system or application.

*Environment* - The aggregate of external procedures, conditions, and objects that affect the development, operation, and maintenance of a system.

*Information Security Policy* - The aggregate of directives, regulations, rules, and practices that regulate how an organization manages, protects, and distributes information. For example, the information security policy for financial data processed on DOD systems can be contained in public law, executive orders, DOD directives and local regulations. The information security policy lists all the security requirements applicable to specific information.

*Information System (IS)* - Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage,

manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

*Information Technology (IT)* - The hardware, firmware, and software used to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

*Information Technology Security (ITSEC)* - Protection and maintenance of confidentiality, integrity, availability, and accountability.

*Risk Assessment* - Process of analyzing threats to and vulnerabilities of an IT system, and the potential impact that the loss of information or capabilities of a system would have on national security and using the analysis as a basis for identifying appropriate and cost-effective countermeasures.

*Risk Management* - Process concerned with the identification, measurement, control, and minimization of security risks in IT systems.

*Security* - Measures and controls that ensure confidentiality, integrity, availability, and accountability of the information processed and stored by a computer.

*Security Policy* - The set of laws, rules, and practices that regulate how sensitive or critical information is managed, protected, distributed, and stored.

*Security Requirements* - Types and levels of protection necessary for equipment, data, information, applications, and facilities to meet security policy.

*Threat* - The capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an AIS, site, application, or network.

*Validation* - Determination of the correct implementation in the completed IT system with the security requirements and approach agreed upon by the users, acquisition authority, and DAA.

*Verification* - The process of determining compliance of the evolving or existing IT system specification, design, or code with the security requirements and approach agreed on by the users, acquisition authority, and DAA.

## Annotated Bibliography

Altiris. (2006). *Documentation*. <http://www.altiris.com/support/documentation.aspx>.

This website has multiple documentation in support of the Altiris products.

Hercules 3.51 Operator Training. (2004). Citadel Security Software Inc. Dallas Texas.

The manual was used to illustrate functionality for local system administrators. This document gives you the basics of each thing that can be performed with Hercules.

REM Deployment Guide. (2004). *The Security Integrator Guide*. Deploying REM within Your Enterprise. eEye Digital Security. Aliso Viejo, California.

This guide provided instructions to on how to integrate with third-party applications, and how to automate certain processes.

REM Management Guide. (2004). *The Security Manager Reference Guide*. Using your REM Deployment and Operations Team. eEye Digital Security. Aliso Viejo, California.

This guide is intended for network security administrators and managers who are familiar with security concepts, and who have experience in performing administrative tasks. It provides an in-depth analysis and instruction on managing REM.

REM Operation Guide. (2004). *The Security Operator Reference Guide*. Using your REM system to secure your environment. eEye Digital Security. Aliso Viejo, California.

The install team to provide the required over the shoulder training used this guide. After REM was successfully installed and configured, the guide was utilized for familiarization of basic tasks that would be performed on a daily basis.

Retina. User Manual. (2004) *Retina Network Security Scanner rev 5-51*. eEye Digital Security. Aliso Viejo, California.

This manual is intended for network security administrators who are responsible for using Retina. The install team to provide the required over the shoulder training used this guide.

Hercules ver. 3.51. (2005). *User Guide Hercules ver. 1*. Citadel Security Software Inc. Dallas, TX.

This document provides all procedures for users to operate the Hercules systems. It gives detail information on all options of the program. The install team to provide the required over the shoulder training used this guide.

Hercules ver. 3.51. (2005). *Installation Guide ver. 1*. Citadel Security Software Inc. Dallas, TX.

This document guides an installer through the whole process of installing Hercules. The install team used this guide during the initial development of the Hercules Servers being deployed.

## References

DODD 8500.1 Information Assurance, October 24, 2002

DODI 8500.2 Information Assurance Implementation, February 6, 2003

CJCSM 6510.01, Defense-In-Depth: Information Assurance and Computer Network Defense, March 25, 2003

National Security Agency, Information Assurance Technical Framework (IATF), Release 2.0.1, September 1999

NSTISSP No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, January 2000

National Security Agency (NSA) Security Guides for Windows

NIST Spec Pub 800-23 Guidance to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, August 2000

DODI 5200.40 DOD Information Technology Security Certification and Accreditation Process (DITSCAP), December 30, 1997

DODI S-3600.2 Information Operations (IO) Security Classification Guidance, August 6, 1998

DODD C-5200.5, Communications Security (COMSEC) (U), October 6, 1981

DISA Instruction 240-115-3, Communication Security

DOD 5400.7-R, DOD Freedom of Information Act Program, September 1998

DOD 5200.1-R, Information Security Program, January 1997

DISAI 630-230-19, DISA Information Systems Security Program, July 1996

DISA Instruction 240-115-3, Communications Security, July 1992.

Army 9AR 25-2, Information Assurance, November 2003

CJCSM 6510.01C, Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), March 2003

*Note: All the above instructions are DOD policies and procedures for implementing any type of systems on a DOD network. As installers we must be familiar with and ensure that all the*

*policies listed above are adhered to. One can look up these policies if they have access to a .mil network and of course have the authorization, i.e. PKI certificate to get in.*

## Work Cited

- Altiris. (2004). Altiris Agent 6.1 SP1 for UNIX and LINUX & MAC Product Guide. Retrieved 5/20/2006, from [http://www.altiris.com/upload/altirisagentlinuxunix\\_002.pdf](http://www.altiris.com/upload/altirisagentlinuxunix_002.pdf).
- Hercules User Manual. (2005). *User Guide Hercules ver. 1*. Citadel Security Software Inc. Dallas, TX.