

UNCLASSIFIED

AD NUMBER
ADB263640
NEW LIMITATION CHANGE
TO Approved for public release, distribution unlimited
FROM Distribution authorized to U.S. Gov't. agencies only; Proprietary Information; Nov 1999. Other requests shall be referred to U.S. Army Medical Research and Materiel Command, 504 Scott Street, Fort Detrick, MD 21702-5012
AUTHORITY
USAMRMC ltr, 5 Jun 2002

THIS PAGE IS UNCLASSIFIED

AD \_\_\_\_\_

Award Number DAMD17-99-C-9001

TITLE: Defense Healthcare Information Assurance Program

PRINCIPAL INVESTIGATOR: Archie Andrews, Jack Stinson, et. al. \_\_\_\_\_

CONTRACTING ORGANIZATION: Advanced Technology Institute  
North Charleston, South Carolina 29418

REPORT DATE: November 1999

TYPE OF REPORT: Annual

PREPARED FOR: Commanding General  
U.S. Army Medical Research and Materiel Command  
Fort Detrick, Maryland 21702-5012

DISTRIBUTION STATEMENT: Distribution authorized to U.S. Government agencies only (proprietary information, Nov 99). Other requests for this document shall be referred to U.S. Army Medical Research and Materiel Command, 504 Scott Street, Fort Detrick, Maryland 21702-5012.

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision unless so designated by other documentation.

20010223 095

## NOTICE

USING GOVERNMENT DRAWINGS, SPECIFICATIONS, OR OTHER DATA INCLUDED IN THIS DOCUMENT FOR ANY PURPOSE OTHER THAN GOVERNMENT PROCUREMENT DOES NOT IN ANY WAY OBLIGATE THE U.S. GOVERNMENT. THE FACT THAT THE GOVERNMENT FORMULATED OR SUPPLIED THE DRAWINGS, SPECIFICATIONS, OR OTHER DATA DOES NOT LICENSE THE HOLDER OR ANY OTHER PERSON OR CORPORATION; OR CONVEY ANY RIGHTS OR PERMISSION TO MANUFACTURE, USE, OR SELL ANY PATENTED INVENTION THAT MAY RELATE TO THEM.

### LIMITED RIGHTS LEGEND

Award Number: DAMD17-99-C-9001

Organization: Advanced Technology Institute

Those portions of the technical data contained in this report marked as limited rights data shall not, without the written permission of the above contractor, be (a) released or disclosed outside the government, (b) used by the Government for manufacture or, in the case of computer software documentation, for preparing the same or similar computer software, or (c) used by a party other than the Government, except that the Government may release or disclose technical data to persons outside the Government, or permit the use of technical data by such persons, if (i) such release, disclosure, or use is necessary for emergency repair or overhaul or (ii) is a release or disclosure of technical data (other than detailed manufacturing or process data) to, or use of such data by, a foreign government that is in the interest of the Government and is required for evaluational or informational purposes, provided in either case that such release, disclosure or use is made subject to a prohibition that the person to whom the data is released or disclosed may not further use, release or disclose such data, and the contractor or subcontractor or subcontractor asserting the restriction is notified of such release, disclosure or use. This legend, together with the indications of the portions of this data which are subject to such limitations, shall be included on any reproduction hereof which includes any part of the portions subject to such limitations.

THIS TECHNICAL REPORT HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION.

---

---

---

---

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE November 1999	3. REPORT TYPE AND DATES COVERED Annual (15 Oct 98 - 15 Oct 99)		
4. TITLE AND SUBTITLE Defense Healthcare Information Assurance Program		5. FUNDING NUMBERS DAMD17-99-C-9001		
6. AUTHORS Archie Andrews, Jack Stinson, et. al.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Advanced Technology Institute North Charleston, South Carolina 29418		8. PERFORMING ORGANIZATION REPORT NUMBER ATLIPS 88-01		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Medical Research and Materiel Command Fort Detrick, Maryland 21702-5012		10. SPONSORING/MONITORING AGENCY REPORT NUMBER		
11. SUPPLEMENTARY NOTES  Distribution authorized to U.S. Government agencies only (proprietary information, Nov 99). Other requests for this document shall be referred to U.S. Army Medical Research and Materiel Command, 504 Scott Street, Fort Detrick, Maryland 21702-5012.				
12b. DISTRIBUTION CODE				
13. ABSTRACT (Maximum 200 words) This Annual Report covers the activities and accomplishments of the Defense Healthcare Information Assurance Program (DHIAP) for the period 15 October 1998 to 15 October 1999. It describes in detail the work completed or nearing completion, the Technical Assessment work and the Prototype Design work. Work that is still in progress or just beginning, such as Demonstration and Technology Transition, is summarized. The Technical Assessment work describes the methods applied in the Information Security Evaluations (ISE) to include site selection, site evaluation preparation, and methodology applied. The reports detailing methodology as well as the observations and recommendations from the evaluations are included as appendixes to this report. Recommendations to extend the methodology to include risk identification and site-directed evaluations are included in the conclusions. The Prototype Development work is described to include requirement analysis, system selection, and prototype evaluation. White papers describing emerging technology research initiated but not yet completed are included as appendixes to the report. Appendixes also include the preliminary design reviews briefings, recommended demonstration equipment configurations, a detailed report on the Survivability Simulator work, and the demonstration plan guiding the laboratory demonstration.				
14. SUBJECT TERMS Information Security, Information Technology, Information Assurance, RADIUS, Computer Security, Healthcare Information Systems		15. NUMBER OF PAGES 95		
		16. PRICE CODE		
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT Unlimited	

NSN 7540-01-280-5500  
(Rev 2-89)

Computer Generated

STANDARD FORM 298

Prescribed by ANSI Std Z39-

**FOREWORD**

Opinions, interpretations, conclusions, and recommendations are those of the author and are not necessarily endorsed by the U.S. Army.

~~(S)~~ Where copyrighted material is quoted, permission has been obtained to use such material.

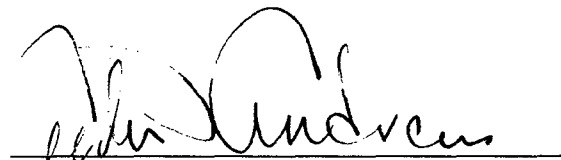
~~(S)~~ Where material from documents designated for limited distribution is quoted, permission has been obtained to use the material.

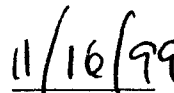
~~(S)~~ Citations of commercial organizations and trade names in this report do not constitute an official Department of the Army endorsement or approval of the products or services of these organizations.

~~(S)~~ In conducting research using animals, the investigator(s) adhered to the "Guide for the Care and Use of Laboratory Animals", prepared by the Committee on Care and Use of Laboratory Animals of the Institute of Laboratory Animal Resources, National Research Council (NIH Publication No. 86-23, Revised 1985).

~~(S)~~ For the protection of human subjects, the investigator(s) have adhered to the policies of applicable Federal Law 32 CFR 219 and 45 CFR 46.

~~(S)~~ In conducting research utilizing recombinant DNA technology, the investigator(s) adhered to current guidelines promulgated by the National Institute of Health.

  
Principal Investigator

  
Date

**Table of Contents**

<b>1. INTRODUCTION</b>	<b>5</b>
1.1 Technical Assessment	5
1.2 Prototype Development	5
1.3 Demonstration	5
1.4 Technology Transition	5
<b>2. BODY</b>	<b>6</b>
2.1 Technical Assessment Task	6
2.2 Prototype Development Task	10
2.3 Demonstration Task	15
2.3 Technology Transition Task	15
<b>3. CONCLUSIONS</b>	<b>16</b>
<b>4. REFERENCES</b>	<b>18</b>
<b>5. APPENDICES</b>	<b>19</b>

## **1. Introduction**

The objective of the Defense Healthcare Information Assurance Program (DHIAP) is to ensure that clinical and other health-related data of Department of Defense active duty personnel and other beneficiary populations are readily accessible, but only as authorized. The DHIAP program will:

- Evaluate installed medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities,
- Validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems, and
- Implement security solutions for evaluation within the military-civilian medical community.

The demonstration prototypes will assist in defining a long-term program that will provide the flexibility to respond to a changing threat, maintain information assurance continuity with the civilian healthcare component, and respond to military requirements for information and operational security.

DHIAP consists of four major areas of work: Technical Assessment, Prototype Development, Demonstration, and Technology Transfer. The work of each is summarized below.

### **1.1 Technical Assessment**

A government-contractor team composed of system security and healthcare experts will perform on-site technical evaluations of selected military sites to reveal healthcare system security issues and site security requirements. The methodology they will use is called the "Information Security Evaluation" (ISE).

### **1.2 Prototype Development**

Design and development of prototype security components to be installed and operated during the Demonstration task will be based on the findings of the Technical Assessment's site evaluations. Key components of successful prototype development and testing are this task's supporting efforts of Requirements Analysis and Emergent Technology Research.

### **1.3 Demonstration**

The realization of the design and testing efforts will be demonstrable improvements to information security at selected healthcare sites. This demonstration will include both applying and integrating the required technology with the functional healthcare system and providing recommendations for the policies, procedures, and methodologies required to operate the secured system.

### **1.4 Technology Transition**

An important objective of the program is to transition the technology, policies, and procedures to an operational healthcare environment. Establishing the test beds at operational military sites and enhancing security is a preliminary requirement to meeting this objective.

## 2. Body

The work completed in the first year of the DHIAP program is presented in this section. A presentation of each major area of work, or "task," begins with a brief summary of the work performed during the year. Immediately following, for each major "effort" of the task, is a presentation of the Methods used to perform the work and a Discussion of any issues, problems, or major discoveries that arose during the work. Finally, there is a brief recap of the direct Result of completing the effort.

### 2.1 Technical Assessment Task

The Technical Assessment Task addresses the first DHIAP objective,

**Evaluate installed medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities.**

Work began with nomination of candidate sites and selection of the MTFs that would participate in the information security evaluation. Concurrent with this effort was a preparation phase in which the DHIAP team members planned how to conduct the site evaluations and received training in SEI's Information Security Evaluation (ISE) methodology. Next, the team performed evaluations at the MTF sites. Following analysis of knowledge gained about each site, the team provided the site with detailed findings resulting from the review and recommendations for immediate and longer-term action. As a final step, the team merged and analyzed the findings of both ISEs and drafted a Composite Report of ISE results and recommendations.

The methods and accomplishments of the four major Efforts of the Technical Assessment task are summarized in **Figure 1** and in the paragraphs that follow. Appendix A provides a more detailed description of the work performed during the Technical Assessment task, as well as some specific materials that were used in conducting ISEs.

#### Site Selection Effort

**Methods/Discussion:** ISE activity began with nomination of candidate MTF sites and selection of the sites that would actually participate. TATRC nominated a number of representative sites, explained the incentive for the nominated sites to participate, and requested initial site information to screen the sites down to a representative sample. The request for information took the form of a Preliminary Survey used to gather basic information about the nominated sites' staff, installed systems, existing policy, current training, and current practices. The Site Selection process is defined in greater detail in Appendix A-1; Appendix A also contains copies of the Preliminary Survey form used in this step and the Site Initial Overview Briefing that was used with the selected sites.

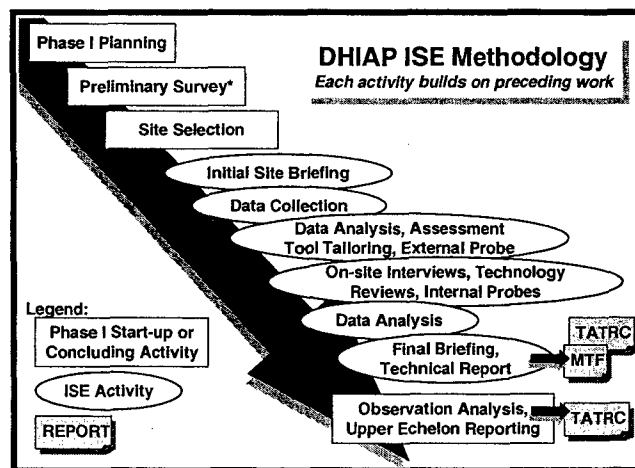


Figure 1 – DHIAP ISE Methodology



**Result:** Based on responses to the Preliminary Survey, TATRC, working with the DHIAP contractors, selected two MTFs to be initially evaluated in the ISE. The selected sites were considered to be representative of the Army MTFs, a Regional Medical Center and a Community Hospital. Because they are in the same region, rather than disparate MTFs, the ISE findings and recommendations should be generally applicable on a regional basis.

**Site Evaluation Preparation Effort**

**Methods/Discussion:** Site Evaluation Preparation, performed concurrently with Site Selection, prepared the materials and general plan of work for performing each MTF’s security evaluation. Since the evaluations would be conducted according to the Information Security Evaluation (ISE) methodology that had been developed by the Software Engineering Institute's CERT Coordination Center, the first significant activity was for the DHIAP team to adapt the ISE approach to fit the needs and scope of DHIAP’s site evaluations.

The ISE process for identifying vulnerabilities in MTFs was designed to be flexible, allowing it to be applied in a variety of domains. In fact, SEI has more than six years of experience delivering ISEs in many domains and has refined the process over this time for maximum flexibility. For DHIAP Phase I, evaluation team members with medical domain expertise were included on the evaluation team, the ISE process was adapted to the MTF environment, and survey questionnaires were tailored for the sites’ specific mission and IT infrastructure. The number and content of interviews with MTF staff members were also tailored to each MTF.

**Figure 2** provides an overview of the type of adaptation made to the ISE approach. While the overall categories of interview subjects were the same for all groups, the team realized that the interviewees’ roles at

the site and exposure to various operational norms made it important to emphasize some categories with one group, others with another group. For example, the team would emphasize perceptions of security policy and remote dial-in capabilities with the medical staff, but emphasize security implementation in application systems and on the network

Group	Typical Group Participants	Interview Areas of Concentration	
Medical Staff	Physicians (e.g., Family Practice, Internists, Pathologists, Oral Surgeons)	FOR BOTH INTERVIEWS	
Clinical Support Staff (Application Users)	Nurses Laboratory Technicians Pharmacy Technicians Radiology Technicians	1 - Security Policy 3 - Physical Security 5 - Organizational Issues 7 - Security Violation P&P 9 - Network/System Security	2 - External Connectivity 4 - Assets/Threats 6 - Security Implementation 8 - Services
Technical Area Managers	Network Managers LAN Managers Security Managers	1 - Security Implementation 3 - Security Policy 5 - Vendors/Contractors 7 - Physical Security 9 - External Connectivity	2 - Network/System Security 4 - Security Violation P&P 6 - Assets/Threats 8 - Organizational Issues
Support Staff (Systems, Network, Patient Administration)	Information Systems Specialists Patient Records Staff Medical Records Staff	1 - Security Policy 3 - System/Network Security 5 - External Connectivity 7 - Organizational Issues	2 - Security Implementation 4 - Security Violations 6 - Physical Security 8 - Assets/Threats
System / Network Technical Leads	LAN Specialist Network Specialist Systems Trainer Application Support Specialists Help Desk Staff	1 - Security Implementation 3 - Security Policy 5 - Vendors/Contractors 7 - Physical Security 9 - External Connectivity	2 - Network/System Security 4 - Security Violation P&P 6 - Assets/Threats 8 - Organizational Issues
Chief, Information Management	Chief Information Officer	1 - Security Policy 3 - Organizational Issues 5 - Vendors/Contractors 7 - Security Implementation 9 - External Connectivity	2 - Assets/Threats 4 - Security Violations 6 - Physical Security 8 - Network/System Security 10- Services

**Figure 2 – Site Interview Groups / Subjects**

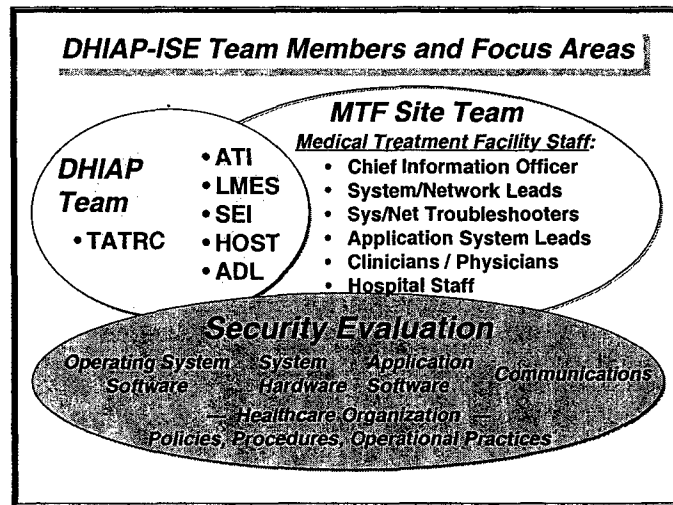
with the technical staff. Based on the adaptations, interviews would focus on the categories where MTF participants had the most knowledge.

The DHIAP evaluation materials were designed to capitalize on the strengths of the ISE process.

- The ISE is a vulnerability evaluation that reveals both organizational and infrastructure weaknesses. The process uses interviews to elicit the perspectives of the information technology staff and the medical staff. The interviews, along with an examination of the organization’s policies, provide insight into the organizational issues that can affect security. The technical examination of the organization’s computing infrastructure provides insight into the technology vulnerabilities that can affect security.
- Another important strength of the ISE process is its flexibility. The ISE process and its artifacts are tailored to an organization, allowing for differences in the organizational structures and technology bases of organizations. Tailoring the process ultimately means that the evaluation team is assured of looking at relevant parts of the organization and infrastructure, increasing the likelihood that they will identify the major security issues.

ISEs are designed to identify weaknesses across an organization and in its infrastructure, not to be in-depth analyses of all weaknesses that are identified. While the evaluation would identify areas for improvement within the MTFs, it would not generate enough information to formulate detailed requirements for the improvement areas. For this reason, the team would plan to subsequently perform certain “targeted” requirements elicitation activities to gather additional information that would be needed for MTFs and TATRC to understand the specific nature or extent of certain ISE findings.

**Figure 3** summarizes (under the “Security Evaluation” heading) the major focus areas of DHIAP’s ISE process; it also indicates the organizations included on the DHIAP evaluation team, and lists the types of staff members that each MTF would be expected to contribute to the Site Evaluation effort. A second major activity of this effort was to name (based on each ISE activity’s need for technical, healthcare, and/or management skills) specific DHIAP team members who should perform each activity and outline the team’s expectations for MTF staff participation in each activity.



**Figure 3 - DHIAP ISE Team Members / Focus Areas**

**Result:** The tailoring of SEI’s more generic ISE surveys assured that the evaluation approach used in DHIAP would closely fit the needs and scope of the program’s security evaluation requirement. The staffing analysis and assignment completed in this task assured that the DHIAP team, a group of highly qualified individuals from industry, academia, and the government, each with extensive experience in information science, information security, computer systems, and/or hospital administration, were deployed in the most efficient and effective manner for conducting ISEs at the MTF sites.

### Site Evaluation Effort

**Methods/Discussion:** The DHIAP evaluation effort examined each selected MTF to understand the current state of information security as practiced there. Each facility evaluation followed the process and general timeline that is shown in **Figure 4**. Note that the steps of the process described in this section are discussed in greater detail in Appendix A-2. Following the end of work at an MTF, the mass of data collected during the evaluations was analyzed by the combined government/contractor team and grouped into actionable areas dealing with management vs. technical issues. While the sites could directly address some of the recommendations, accomplishing others required coordination across the sites' command hierarchy.

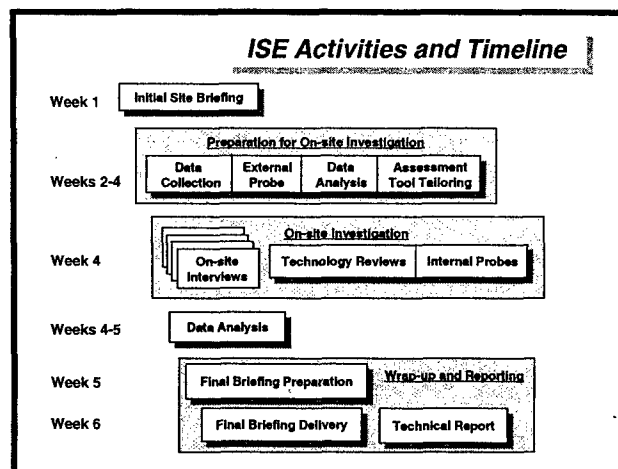


Figure 4 - ISE Activities and Timeline

**Result:** Each ISE concluded with several forms of feedback to the site, as follows. Certain observations, along with recommendations for specific technical issues, were provided to appropriate MTF staff during the course of the evaluation. A Site Vulnerability Assessment Final Briefing outlined the team's observations and recommendations of instances where site information was found vulnerable to exposure due to organizational, policy, personal, or technology issues. The briefing was specific to the MTF site and was provided to MTF leadership, the MTF's Chief Information Officer (CIO), selected staff of the Information Management group of the MTF, and all MTF staff members who had participated in the ISE process. These briefings are proprietary to the sites and have been excluded from this report. Subsequent to this briefing, a report providing technical details of importance to the system and network administrators was provided to the CIO at the MTF. These technical reports also contain information proprietary to the sites and have been omitted from this report.

### "Composite Report on Evaluations" Effort

**Methods/Discussion:** Following completion of the scheduled Phase I ISEs, the DHIAP team clustered the observations from each site in various ways to identify information threats and vulnerabilities common to all sites evaluated. They analyzed the observations and recommendations developed during all of the ISEs to develop a "Composite Report" of observations and associated recommendations. The report will outline the types of vulnerabilities evident in the military MTFs and MTF use of policies and procedures for protecting confidential information, and will provide the DHIAP team's recommendations for actions to address the vulnerabilities.

**Result:** The DHIAP team has completed all Information Security Evaluations planned for the Technical Assessment task of Phase I. The goals of performing the ISEs in MTFs were to develop a baseline of the current state of practice of information assurance at the MTF, identify organizational and technology issues for a subsequent improvement effort by the DHIAP team, provide immediate feedback assistance to the evaluated site, and develop programmatic issues to

advise and assist responsible agents within DoD. The ISE process achieved this goal, as many organizational and technology issues were identified in the evaluation of each MTF. The team provided detailed feedback to the MTFs who participated in the ISEs and to TATRC, and analyzed all information gathered to determine vulnerabilities common to many sites vs. those that seemed to be site-specific. The DHIAP team performed several wrap-up activities to conclude their Technical Assessment work:

- Drafted a Composite Report of vulnerabilities and recommendations, grouping the material based on whether the issue could be resolved at the local MTF level or had to be addressed at higher echelons of command. The Composite Report is undergoing final review and is scheduled for completion by November 30, 1999. A working draft of the Composite Report including the Introduction, ISE Process, and Observations and Recommendations sections is attached as Appendix F. The final version of the Composite Report will include, in addition to these sections, an Executive Summary and a section on Conclusions and Recommendations.
- Used knowledge gained from completing the Phase I Assessments to begin the Requirements Analysis Effort of Phase I's Prototype Development Task.

## **2.2 Prototype Development Task**

The Prototype Development Task addresses the second DHIAP objective,

**Validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems.**

Initial work involved building a set of candidate requirements based on analysis of the vulnerabilities identified during the Technical Assessment task. These requirements were further refined during a requirements-gathering effort conducted by representatives of the DHIAP team and staff from the MTFs that had participated in an ISE. The DHIAP team then used the Army's security requirements (as reflected in MTFs' aggregate requirements, the Department of the Army directive<sup>1</sup>, and the Internet Engineering Task Force (IETF) specification<sup>2</sup>), a vendor search, and their extensive networking experience as the basis for recommending the hardware and software components for the prototype demonstration. In the final Prototype Development activity completed during Year 1 of the program, the team established a "distributed laboratory." The selected components were installed according to manufacturers' recommendations in labs at ATI and LMES, software was loaded, and configurations were developed to meet Army-directed objectives. The methods and accomplishments of the four major efforts of the Prototype Development task are provided below.

### ***Requirements Analysis Effort***

**Methods/Discussion:** A number of MTF vulnerabilities were identified during the ISE process. The DHIAP Team worked to prioritize vulnerabilities as candidates for prototype development using such criteria as relevance to MTF needs, relevance to TATRC mission, authority of the MTF to direct and implement change, cost, complexity, existence of a solution, and the team's opinion of how best to make a difference in information security at the MTF. This initial prioritization of potential options was combined with on-site analysis of requirements and working sessions with the technical staff at the regional testbed site to ensure that technical and

operational issues were identified. It was decided that the implementation of the regional medical center would be mirrored at the community hospital level.

The Team's initial proposal to the MTFs was to secure e-mail service with secure socket layer (SSL) sessions for protection of information in transit from remote users to the MTF computing environment. The MTFs responded that they were on a path to implement SSL for electronic mail, but that they needed technical assistance to comply with Army directive for remote access dial-in users standard (RADIUS)<sup>1</sup>. Implementing this capability provides the site with much improved identification and authorization of the dial-in users of hospital systems.

**Result:** The MTFs and the DHIAP team agreed that the Prototype Demonstration would implement a RADIUS-compliant server capability that would fulfill the Army's requirement for identification and authentication of dial-in users. **Figure 5** summarizes the capabilities initially required by the Army directives and indicates the capabilities of the solution proposed by the DHIAP team. In addition, the graphic lists "derived" requirements that were added based on input gathered from DDEAMC and WACH during the Requirements Analysis meetings held at their sites.

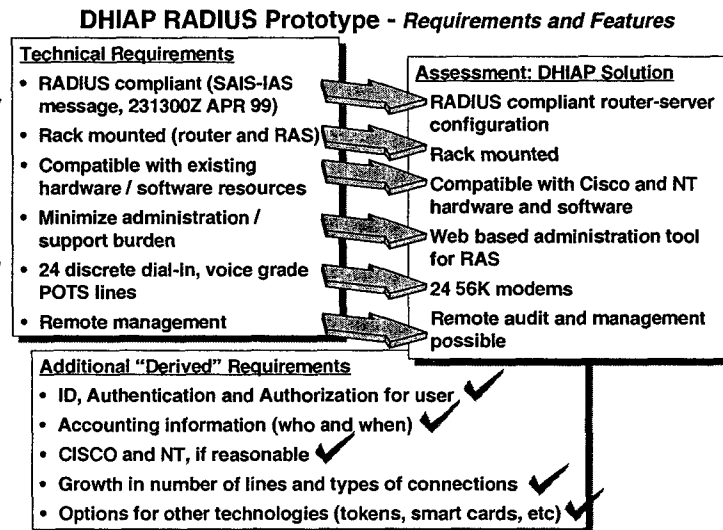


Figure 5 – RADIUS Requirements and Features

**System Selection Effort**

**Methods/Discussion:** The DHIAP Team studied the Army RADIUS guidance<sup>1</sup> and the RADIUS standard<sup>2</sup>; where additional information was required, the Team worked closely with TATRC to get clarification. Armed with an understanding of the letter of the requirement, the Team searched the WWW, technical journals, and personal contacts within the router and computer security industry for compliant components. The candidate technologies considered for the RADIUS solution are listed in **Figure 6**, along with capabilities that were considered significant technical shortcomings. Factors considered in narrowing the technology choice included: compatibility with the

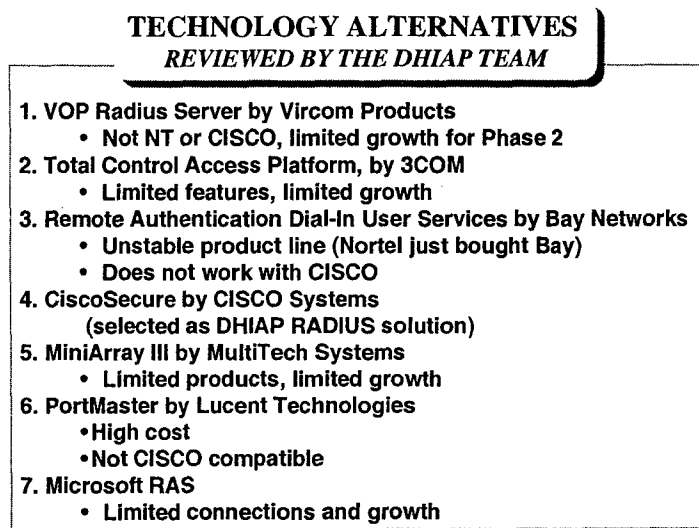


Figure 6 – Technology Alternatives Reviewed

MTFs' existing CISCO routers and Windows NT hardware, capability to support web-based administration, support for remote auditing, and cost to the MTF of follow-on support. It was also important that the selected technology provide a path to support growth in the number of lines and types of communications as well as options to support such other technologies as tokens and smart cards.

**Result:** Based on reviewing the list of compliant components, knowing the technical skills available within the MTF Information Management Divisions, and knowing the components already in operation at the MTFs, the Team recommended the Cisco 3600 series router and an Intel-based computer running Windows NT Server and CiscoSecure as the technical solution for the RADIUS prototype. Specific components of DHIAP's RADIUS are listed in **Figure 7**.

It should be noted that CiscoSecure for Windows NT offers a number of features essential to the program's goals, including:

- Supports remote management and a common user interface using a built-in web server with an HTML interface
- Reduces user burden by authenticating against the Windows Domain Name/Password Database
- Will support growth through its use of third-party token-card servers (SecurID, Enigma Logic, SecureNet, and any hexadecimal X.909).
- Supports TACACS and RADIUS, allowing both to run simultaneously
- Supports logging and auditing

**Figure 8** depicts a typical site installation using the components selected for RADIUS. The resulting recommendations were briefed to the test sites in August for their review and to identify and resolve open issues. A copy of the briefing and a summary of the feedback received from each site are included as Appendix B.

### ***Emerging Technology Research Effort***

**Methods/Discussion:** Based on the findings of the Technical Assessments and knowledge of emerging technology and policies, the DHIAP team proposed three areas of research pertinent to the security issues facing the MTFs immediately or in the near future. Those three areas of investigation and research are: Public Key Infrastructure, Development of a Trust Model, and

### **RADIUS Hardware / Software Solution**

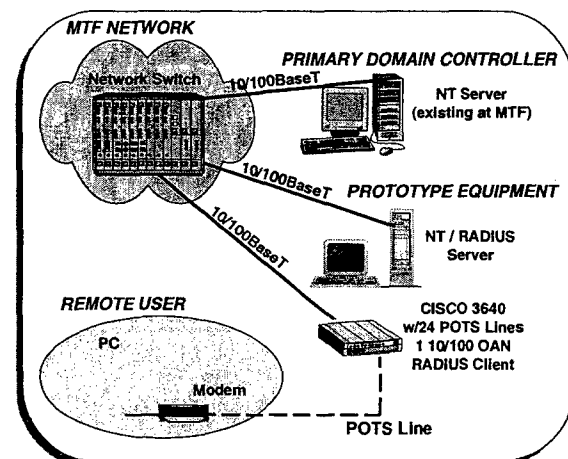
#### **HARDWARE**

- **Compaq AP500**
  - PIII 500 Mhz
  - 128 Mbytes
  - 9 Gbytes SCSI HD
  - 12 Gbyte DAT Drive
  - 17 " Monitor
  - 56k Modem
- **Cisco 3640 Router**
  - 24-56k Modems
  - 10/100 Mbit Ethernet Card
  - 16 Mbytes
- **APC Smart-UPS 1400**
- **Compaq 7000 Series Rack**

#### **SOFTWARE**

- **NT Server 4.0**
  - Service Pack 4.0
  - Y2K Patches
  - IIS - Internet Information Services
  - CiscoSecure ACS 2.3
  - APC PowerChute Plus
- **Cisco IOS 12.0**
  - Configuration File

**Figure 7 – RADIUS Hardware/Software Components**



**Figure 8 – RADIUS Prototype Design**

Remote Administration. Each of these research areas is described in white papers included in as Appendices C-1 through C-3.

**Result:** This investigation/research work is ongoing. The papers resulting from this investigation/research are scheduled for completion by December 1999.

### ***System Design Effort***

**Methods/Discussion:** The selected components were purchased and delivered to DHIAP technical teams at Lockheed Martin Energy Systems in Oak Ridge TN and the Advanced Technology Institute in North Charleston SC. Each site established a development lab and installed the hardware and software. None of the installations went smoothly. However, because the challenges they introduced were indicative of the types of issues that would later arise at various MTFs, the team was able to gain experience with many types of difficulty and use this knowledge to harden, improve, or make flexible the technical plans and instructions that would later be used with the MTFs.

Examples of the types of issues addressed in the initial installations include the following:

- Documentation for CiscoSecure and the Cisco router was not conducive to a rapid installation and configuration. Input was obtained from in-house and consulting staff members with extensive Cisco experience.
- Some hardware components were temporarily substituted by the vendor pending availability of ordered components (e.g., the modem circuit board for the router).
- Each site created a small local area network (LAN) consisting of the router, the server running CiscoSecure, one or more additional host systems, and a network hub. Because the router does not include a monitor, its display was directed to a window on the server.
- Because of Oak Ridge National Laboratory's security policy, the lab in Oak Ridge included a closed circuit, dial-tone/ring generator.

**Result:** Use of the distributed laboratory approach provided the team with a substantial boost in productivity. Team members were able to work in parallel on different aspects of the problems and share breakthroughs as the effort progressed. This resulted in "leap-frog" progress, each team building on the successes of the other. Such advances would not have occurred with either a single team working on a single suite of equipment or multiple teams working in isolation.

On October 15, the Team was able to dial the router, authenticate a user via the server / CiscoSecure, and direct that user to a pre-determined host on the network. This milestone demonstrated satisfaction of the requirement for a user to log on and establish a telnet session with a host (in the demonstration UNIX system access emulated actually accessing an MTF's Composite Health Care System). An additional security feature of this connection is the provision of a proxy IP address by the router. The IP address that the remote user sees is not real and, therefore, provides no useful mapping information for a future attack. Similarly, the simulated CHCS host knows only that the user comes from the router.

Further configuration and testing, planned as part of this demonstration but scheduled to occur after the October 15 timeframe of this report, is required to demonstrate a dial-up to one site with authentication at another site. This will satisfy the requirement to demonstrate centralized authentication, either by command decision or as alternative in the event of local authentication server failure.

***Prototype Evaluation Effort***

**Methods/Discussion:** Prior to installing the prototype in an operational environment, it is essential to ensure that the components will operate effectively within the existing MTF systems. To satisfy that constraint a multi-stage evaluation effort was accomplished.

In the first stage of the evaluation, the proposed demonstration system was subjected to review by a group of system experts independent of the design team. Personnel from SEI reviewed the system design with the assistance of graduate students from Carnegie Mellon University. That review entailed understanding the system requirements of the infrastructure at an MTF. A model of the healthcare information infrastructure is to be included in a Master's thesis at the Carnegie Mellon University's Information Network Institute. Additionally, the requirement to understand issues surrounding a system's infrastructure supported the need for a simulator able to model and analyze a system's characteristics in terms of security and survivability. Carnegie Mellon's work on development of a simulation capability coupled their DHIAP work with another effort being performed for the US Air Force's Research Laboratory to develop the theory and formal characterization of a simulation capability applicable to issues in the information assurance context. Progress on Carnegie Mellon's security and survivability simulator effort is summarized in a report included as Appendix D.

The second stage of evaluation will begin once the design has been determined to be fundamentally sound and able to satisfy the MTF requirements. Early in DHIAP Year 2, the Team will emulate the essential characteristics of an MTF system infrastructure in a multi-site lab environment in order to understand installation and implementation issues. Since the MTF physical infrastructure consists of UNIX, NT, and VMS systems, the multi-site lab will emulate connection to and from these type devices by configuring its systems to apply the existing communication protocols. Installation in a lab environment will permit aggressive debugging of installation, training, and operational issues prior to arrival at the trial sites for installation and implementation. The plan that guides the demonstration is included as Appendix E.

Demonstration of the RADIUS capabilities in a multi-site lab environment, an important milestone of the lab evaluation step, is scheduled for November 3, 1999, at the ATI facilities. The demonstration will show connection of a dial-in user through the RADIUS configuration with separate devices that include (1) a UNIX system emulating a CHCS telnet connection, and (2) Web server/NT server configured to represent an MTF's exchange web server. The DHIAP team will present the demonstration to an audience planned to include TATRC program managers and the technical staff for the test sites.

Third, after demonstration in the lab, the systems will be installed at the identified test sites to extend the capabilities into an operational environment. The MTFs will be given an initial operational capability (IOC) upon system installation; full operational capability (FOC) will be scheduled for approximately 30 to 45 days following the IOC. The IOC is intended to give the sites an opportunity to become familiar with the capability and to plan for the migration of their user population to the new capability; installation of the IOC will begin the work of DHIAP's Demonstration Task.

**Result:** The prototype evaluation will result in a validation and verification of the design of the demonstration capability for identification, authentication, authorization, and accounting of remote access dial-in users. The first stage, evaluation by an independent group, was completed;



the proposed design appears to be sound and provides improvements in security as well as improvements in capability. The evaluation also leveraged the work required to understand MTF existing system infrastructure with the Air Force laboratory's investment in simulation, in order to make significant advances in developing a simulation capability that will support understanding issues in security and survivability as detailed in Appendix D. The second stage of the evaluation, demonstration in a laboratory environment, if successful will result in the sites' understanding of equipment capabilities and agreement on installation of IOC at their sites. Results of the demonstration will be reported in future DHIAP Quarterly and Annual Reports.

### **2.3 Demonstration Task**

The Demonstration Task addresses the third DHIAP objective,

**Implement security solutions for evaluation within the military-civilian medical community.**

The DHIAP team began this task by defining configurations for the information security components to be installed at each MTF testbed. The work was based on the knowledge of MTF technical environments acquired during ISEs, the results of requirements analysis, and component testing during the Prototype Development effort. The components were ordered, and initial schedules were defined for installation and evaluation.

Work remaining to be done in Year 2 includes installing the components, finalizing plans for performing the demonstration within and across testbed sites, developing the operational and policy guidance documentation of appropriate use of the new technology, and training MTF staff on use of the overall (systems and procedural) use of this Phase I product.

**Methods/Discussion:** Work on this task, which is dependent upon completion of Task 2.2 above, involved initial planning for conducting the real-world demonstration of the DHIAP information protection prototype. Based on results of the prototype installation and testing accomplished in the Prototype Development effort, the system configurations were defined and orders were placed for the hardware and software components to be installed and demonstrated at the Telemedicine and Advanced Technology Research Center at Fort Detrick MD and the two MTFs participating in this effort.

**Result:** Delivery and installation of RADIUS equipment to each MTF and to TATRC is scheduled for November-December, 1999. Specific schedules for installation and initial use of the system will be confirmed during the November 3 demonstration.

### **2.3 Technology Transition Task**

The Technology Transition task is a second component of the Demonstration Task's DHIAP objective to:

**Implement security solutions for evaluation within the military-civilian medical community.**

Since establishing the test beds at operational military sites and enhancing security is a preliminary requirement to meeting this objective, work on this task will begin after the MTF site testbeds have become operational and the DHIAP prototype technologies have been proven. The effort will include providing technical and programmatic advice regarding long-range programs

to provide the flexibility to respond to a changing threat, maintain information assurance continuity with the civilian healthcare component, and respond to military requirements for information and operational security.

### **3. Conclusions**

In addition to accomplishing the DHIAP program work described in Section 2 above, the DHIAP Phase I activities performed in Year 1 have resulted in a number of tangible improvements to protection of information at MTFs. In addition, the work done in each major task has resulted in specific knowledge that will improve the remaining work of the task.

#### ***Technical Assessment***

Technical Assessment activities provided immediate benefits to the sites involved in the ISEs, including the following:

- Vulnerabilities were identified and reported to the sites' leadership and technicians.
- The DHIAP investigators provided immediate assistance in addressing some of the vulnerabilities as they were identified.
- The DHIAP investigators provided limited hands-on training to MTF staff during the course of the evaluation.
- ISE technical recommendations for appropriate responses to vulnerabilities pertaining to the remotely managed systems were forwarded by at least one of the sites to managers of the command-wide systems for action.
- The ISE process and its results increased the MTF Command's overall awareness of security issues.

Through completing technical assessments at the MTFs, the Team was able to make or confirm certain important observations about the ISE process:

- Business Continuity – Business continuity is a major reason why organizations want to evaluate their security. Managers would like to ensure that they are adequately protecting their important information assets.
- Scope of Evaluations – It is important to evaluate both the organization and the technology when performing security evaluations.
- Contextual Nature of Evaluations – How people use and interact with technology is dependent on the given situation. Every MTF visited is noticeably different. To allow for site-specific differences, the evaluation method must be flexible and allow for tailoring. In Phase I, the ISE interviews were tailored for the MTFs that we examined. The technology reviews were tailored for the installed computing infrastructures that we found at those MTFs.
- Expert Delivered Evaluations – Organizations must be actively engaged in the evaluation process if meaningful improvement is to follow. When experts perform an evaluation on an organization, the organization's staff takes a relatively passive role. Our experience leads us to believe that (1) the staff often does not accept the findings of the experts, or (2) they don't

know where to begin to resolve the issues identified by the evaluations. In either case, making subsequent meaningful improvement is a challenge.

- **Decision Support** – Evaluation results must be in a format that enables site personnel to make necessary tradeoffs. Every organization has limited staff and funding. Managers need to understand the implications of organization or infrastructure vulnerabilities in order to make the necessary tradeoffs against other issues and problems that they are facing.

The ISE method for evaluating the security of organizations has many strengths. However, the method needs to be extended in two areas:

- The evaluation needs to include a focus on risks and identifying their relationship to the vulnerabilities that are found. The results of a risk evaluation will allow organizations to see which of their important information assets are at risk; management can then make the tradeoffs that are necessary to help ensure that the organization is in the best possible position to achieve its mission.
- The site being evaluated should be actively involved in the evaluation process, encouraging them to “own” the results and motivating them to act on the recommendations. A “self-directed” type of ISE will assure that organizations are managing and directing the risk evaluation themselves. Even if an organization’s staff does not perform all parts of the evaluation because they lack the skills necessary to do so, they will still be engaged in the process and be directing it. Ultimately, they will be better prepared to leverage the results of the evaluation and improve security of their information assets in meaningful ways.

Any improvements to the ISE process should build on the strengths of the ISE while also addressing its weaknesses. As such, the risk evaluation needs to be a flexible process that evaluates both organizational practices and infrastructure vulnerabilities. The evaluation must place vulnerabilities in a meaningful context for the organization. Vulnerabilities must be linked to the assets that they are placing at risk to show their impact to the organization. This will also allow managers to use the evaluation results and incorporate them into their decision-making processes. The risk evaluation process must be flexible and allow for tailoring to meet the needs of specific sites. Ideally, it should put organizations in a position for meaningful security improvement.

### ***Prototype Development***

Implementation of the RADIUS prototype accomplishes several complementary advances in security capabilities. It will provide improved identification, authentication, and accounting of dial-in users, and will also facilitate controlling users’ access to specific systems. It has presently untapped capabilities to provide additional security to the site. Also, it serves as a focal point to encourage the site to examine and revise its security policies, practices, and user awareness regarding dial-in users, password administration, and access control. Thus, the technology demonstration has not only advanced security capabilities at the MTFs, but it also serves as a forcing function to heighten security awareness at the sites.

The selected system configuration appears to meet the RADIUS requirements and show strong potential to satisfy other ISE vulnerabilities at some future point in the DHIAP program. In addition to controlling remote dial-up users, the demonstration prototype is capable of controlling both users logging on internally and users arriving at the MTF network from the Internet or

MEDNET. The selected configuration will lay the groundwork for creating a single entry point into a defensive perimeter for the MTF information systems. While there is much work to be done in the development and dissemination of policy and the removal of other entry points, the RADIUS capability can be used to show the MTF computer users that a single entry point will increase their information assurance without degrading information accessibility.

The RADIUS solution prototyped in DHIAP Phase I may resolve additional important security issues faced by the MTFs and documented during the ISEs. Although the DHIAP Phase I scope of effort (time, funding, and target deliverables) precluded formally addressing these areas in the demonstration, the team kept these high priority concerns in mind when evaluating the RADIUS components. They are:

- Planned for demonstration in DHIAP I, but not yet tested, is the ability to centrally authenticate users from multiple MTFs. There is some debate among MTF Information Management Division members as to the desirability of doing business this way. The MTF managers need to weigh the operational and organizational impact of controlling of one's own user list against both the risk of loss of local log on due to loss of remote connectivity and the workload of maintaining user access lists. Delivery of the RADIUS capability will be a catalyst for this discussion.
- Although time prohibited confirmation during DHIAP Phase I, it appears that this prototype can be extended to support encrypted sessions, thus protecting patient information while in transit and protecting the extremely sensitive information communicated during remote (central) administration of standard healthcare information systems by higher headquarters and their contractors.
- Future experimentation may also reveal the potential for use of public/private key authentication and session encryption, use of IP sec, and support of virtual private networks.

#### **4. References**

---

<sup>1</sup> R 231300Z APR 99

FM HQ WASHINGTON DC//SAIS-IAS//

<sup>2</sup> URL for the radius IETF standard (rfc 2058): <http://www.ietf.org/rfc/rfc2058.txt>

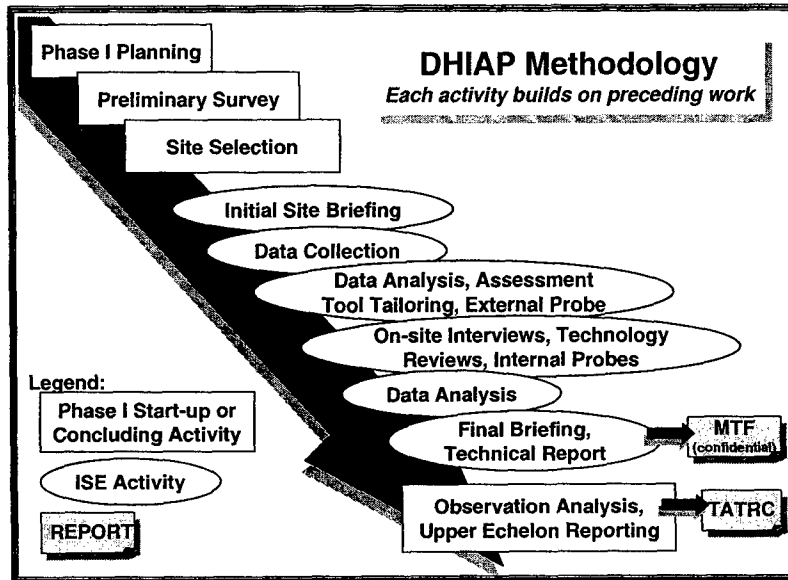
**5. Appendices**

<b><u>APPENDIX</u></b>	<b><u>TITLE</u></b>	<b><u>PAGE</u></b>
A	DHIAP Phase I Technical Assessment Methodology	21
A-1	Site Selection Effort	22
A-2	Site Evaluation Effort	23
Att. 1 to Appendix A	DHIAP Preliminary Survey	26
Att. 2 to Appendix A	Site Initial Overview Briefing Slides	29
B	Report of Preliminary Design Review	31
B-1	Report of RADIUS Preliminary Design Reviews, August 1999	32
B-2	Briefing Used in RADIUS Preliminary Design Reviews, August 1999	40
C	Emerging Technology Research	44
C-1	DHIAP White Papers: Public Key Infrastructure	45
C-2	DHIAP White Papers: Trust-Model Development	47
C-3	DHIAP White Papers: Remote Administration	49
D	Security and Survivability Simulator	51
E	Demonstration Plan	57
F	DHIAP Phase I Composite Evaluation Report – Working Draft	60

**Appendix A – DHIAP Phase I Technical Assessment Methodology**

The methodology used in the Defense Healthcare Information Assurance Program (DHIAP) Information Security Evaluation (ISE) was adapted from evaluation processes initially developed

by the Software Engineering Institute (SEI). This Appendix describes the activities performed in each step of the DHIAP's implementation of the methodology, depicted in **Figure A.1**. In the Figure, the rectangular shapes represent the team's activities to plan and initiate, then conclude, Phase I activities. Oval shapes in the center portion of the diagram identify the major steps of the ISEs that were conducted at military Medical Treatment Facilities (MTFs). As implied by the sequence of shapes along the arrow, from upper left to lower right in the Figure, each activity



**Figure A.1 - DHIAP Methodology**

of the DHIAP Methodology builds on the results of preceding work. Appendices A-1 and A-2 summarize the work performed during the Technical Assessments.

**Appendix A-1 – Site Selection Effort**

**Phase I Planning.** Planning for DHIAP Phase I required identifying participating military Medical Treatment Facilities to identify characteristic system vulnerabilities and participate in demonstrations of tools and techniques to reduce or eliminate the exposure. DHIAP was designed to begin by establishing a baseline of the current state of information assurance in a representative set of military MTFs. That baseline provides the roadmap for the next step in DHIAP Phase I, addressing problems found with current MTF information systems to demonstrate improvements in policy, practices, and technology employed at each participating MTF. Since information derived from the initial set of sites is assumed to represent the problems and issues associated with military MTFs in general, the selection of an initial set of participating sites that were representative of the larger population of MTFs was key to the success of the effort.

**Site Selection.** As the government sponsoring organization for DHIAP ISEs, TATRC nominated specific candidate sites for the study. TATRC sent each nominated MTF a letter explaining the ISE process, its advantages, and the commitment requirements for sites participating in the ISE. Enclosed with the letter was the Preliminary Survey, instructions for completing it, and deadlines.

Based on information in the completed surveys and the sites' willingness to commit the appropriate staff resources, TATRC selected candidate MTFs for Phase I participation. The TATRC sponsor and the DHIAP Principal Investigator visited each of the selected sites to brief the commander and staff on the objectives and requirements for the ISE and its follow-on activities. (A copy of the presentation used at the Site Overview Briefing is included as **Attachment 2** to Appendix A.) They verified the site's commitment to DHIAP and developed the initial plans and schedule for conducting its ISE. During the meeting, MTF senior staff named the individual who would serve as the site's designated ISE "On-site Coordinator," then the group discussed and resolved operational issues and, scheduled the critical dates for the ISE. Site identification was scheduled for completion within sixty days of initiation. Site selection included gaining site commitment to (1) the ISE process and (2) follow-on participation in the demonstration. The DHIAP ISEs were projected to require a minimum of eight weeks elapsed time per site. When possible, concurrent activities were scheduled so that multiple sites could be evaluated in the time allocated. Schedules called for all ISEs to be completed within five months of site selection.

**Preliminary Survey Development.** The military and civilian team members worked together to develop a Preliminary Survey questionnaire for use in profiling the security-related aspects of an MTF's technical and operational environment. It provided a brief background about the study, instructions for completing the survey, named TATRC's point of contact for the study, and included several pages of questions to be answered by site personnel.

The Preliminary Survey, **Attachment 1** to Appendix A, was designed to gather high-level information about the major areas to be covered in an ISE. Types of information covered in the questionnaire include: a profile of the organization's staffing and prior experience; an overview of the facility's systems and networks; information about the facility's policy and actual practice related to security of patient and other sensitive information; and an overview of types of external access that occur in the system's information processing environment.

**Appendix A-2 – Site Evaluation Effort**

**ISE ACTIVITIES: (1) Preparation for On-Site Investigation**

**Initial Site Briefing.** ISE activities began with a meeting at the MTF between DHIAP ISE team leaders and the site’s senior staff to define specific plans for conducting the study, set timeframes, and designate the types of MTF staff who would participate. Following the briefing, MTF personnel arranged staff availability in order to provide specific additional technical and organizational information to the DHIAP team. To improve DHIAP team members’ understanding of unique technical and clinical characteristics of the site, the group reviewed portions of the MTF’s Preliminary Survey responses.

**Data Collection.** At the initial site briefing, the DHIAP team provided a detailed Site Survey to the MTF’s Chief Information Officer (CIO). The CIO, through the On-site Coordinator, arranged for appropriate MTF personnel to provide the requested information and return the completed survey. The Site Survey’s questions had been organized to align with MTF staff responsibility areas; the requested information corresponded to subjects covered by the Preliminary Survey, but in greater detail. Questions covered such subjects as: the hardware and operating systems in use at the site; ownership, content, and support arrangements for the MTF’s computer systems and network; and hardware, software, and configuration of the MTF’s network.

The On-site Coordinator distributed survey sections to appropriate MTF leaders (including administrators of the various computer systems, technical support staff responsible for the office file server, network, and LAN, and administrators for applications such as CHCS, etc.). The staff completed their portions of the Site Survey and returned them to the On-site Coordinator, who reviewed the responses for accuracy and completeness and forwarded them to the DHIAP team.

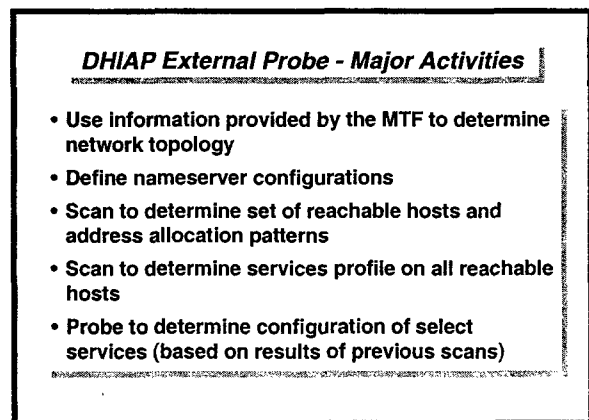
**External Probe.** The ISE team tailored ISE scripts for the External Probe using the Site Survey responses in combination with additional information gathered through coordinating with the MTF’s Information Management leaders. They obtained specific permission from the site to

perform the ISE’s Internet-based probe of MTF networks and systems, then notified site staff and such other interested parties as the Army CERT of the specific day and time that the probe would be performed.

The External Probe used commonly available software tools to identify the types of MTF information that were visible to the public. Major areas addressed by the probe are listed in **Figure A.2**. While the probe’s purpose was to document site-specific information available to anyone accessing the site from the publicly available network, the probe’s scripts and activities were carefully designed to refrain from interrupting or disturbing normal operations.

**Data Analysis and Assessment Tool**

**Tailoring.** Following completion of the External Probe, the team used its results along with information collected via the Site Survey to adapt questions and areas of emphasis for the next ISE activity, the On-Site Investigation. They tailored the methodology’s materials for conducting



**Figure A.2 – External Probe Areas of Coverage**



On-site Interviews to fit the MTF's specific technical characteristics and mapped the interview questions to the staff scheduled for each of the site's interview groups. While the team used the methodology's standard questions "as is" (to assure they covered the same list of relevant areas and used the same phrasing of questions at every ISE site), they adjusted the sequence or emphasis of the questions planned for each interview. The adjustments were designed to assure that (1) subjects were appropriate to the site's technology profile and interview group composition, and (2) the most critical areas of knowledge / concern appropriate for each interview group would be covered in the time allowed. **Figure A-3** below provides some insight into how the ISE investigation areas were sequenced to fit the expertise and areas of concern of the different interview groups.

**ISE ACTIVITIES: (2) On-site Investigation**

**On-site Interviews.** The DHIAP team conducting the On-site Interviews was composed of an Interviewer, an Issue Recorder, an Official Recorder, a Process Recorder and Observers. MTF staff represented the roles listed in **Figure A.3**. The interview process paired certain ISE investigators' skills with appropriate MTF staff groupings (e.g., technicians with technicians, clinically grounded DHIAP team members with MTF clinical staff, etc.).

To protect the interviewees and support a free flow of information, MTF groupings pulled together staff at similar job levels, usually with related or compatible responsibility areas. Participants were always grouped separate from staff at other levels of their line of authority (i.e., Information Management staff were interviewed independently from the IM supervisors, and both were separate from the interview with IM senior management). All

interviewees were asked to honor a policy of non-attribution in which statements made by individual members of an interview group or derived from a group's consensus would not be attributed to either the speaker or the group.

The group interviews were scheduled as 1 1/2 hour sessions, all following the same basic process. The Official Recorder took verbatim notes of MTF staff responses to the questions. To ensure that all required information was obtained, the interview team often used the responses to the scripted questions as the basis for asking additional, non-scripted questions. "Issues" raised during the interview were recorded in public view on white boards or flip charts, were reviewed by the group, and were modified as needed to assure accuracy. While it was rare for all of the planned questions to be covered in a single interview, the team did assure that all questions of the standard methodology were answered by the time that all interviews had been completed. Following completion of interviews conducted on the first day of the On-site Visit, the DHIAP team performed an interim analysis of interview results and adjusted the activities planned for the following day (the Technology Reviews and Internal Probes) accordingly.

Group	Typical Group Participants	Interview Areas of Concentration*	
Medical Staff	Physicians (e.g., Family Practice, Internists, Pathologists, Oral Surgeons)	<b>FOR BOTH INTERVIEWS:</b>	
Clinical Support Staff (Application Users)	Nurses Laboratory Technicians Pharmacy Technicians Radiology Technicians	1 - Security Policy 3 - Physical Security 5 - Organizational Issues 7 - Security Violation P&P 9 - Network/System Security	2 - External Connectivity 4 - Assets/Threats 6 - Security Implementation 8 - Services
Technical Area Managers	Network Managers LAN Managers Security Managers	1 - Security Implementation 3 - Security Policy 5 - Vendors/Contractors 7 - Physical Security 9 - External Connectivity	2 - Network/System Security 4 - Security Violation P&P 6 - Assets/Threats 8 - Organizational Issues
Support Staff (Systems, Network, Patient Administration)	Information Systems Specialists Patient Records Staff Medical Records Staff	1 - Security Policy 3 - System/Network Security 5 - External Connectivity 7 - Organizational Issues	2 - Security Implementation 4 - Security Violations 6 - Physical Security 8 - Assets/Threats
System and Network Technical Leaders	LAN Specialist Network Specialist Systems Trainer Application Support Specialists Help Desk Staff	1 - Security Implementation 3 - Security Policy 5 - Vendors/Contractors 7 - Physical Security 9 - External Connectivity	2 - Network/System Security 4 - Security Violation P&P 6 - Assets/Threats 8 - Organizational Issues
Chief, Information Management	Chief Information Officer	1 - Security Policy 3 - Organizational Issues 5 - Vendors/Contractors 7 - Security Implementation 9 - External Connectivity	2 - Assets/Threats 4 - Security Violations 6 - Physical Security 8 - Network/System Security 10 - Services

\*NOTE: Although all group interviews were designed to cover the same subject matter, the sequence in which subjects were addressed allowed emphasizing certain subjects (see bold print) based on type of staff represented in the interview group.

**Figure A.3 - MTF Interview Summary**

**Technology Reviews and Interviews.** The second day of the On-site Visit emphasized Technology Reviews in which ISE team members used previously obtained information to examine targeted systems. Also, working with the MTF's responsible computer and network system administrators, they examined key security aspects of selected computer systems by examining user permissions and system configurations of the MTF's installed systems and applications. A representative list of the systems examined in this process is included as **Figure A.4**.

**Technology Interviews** were based on site-specific information derived from responses to the Preliminary and Site Surveys, External Probes of the site, and the observations and issues recorded during On-site Interviews.

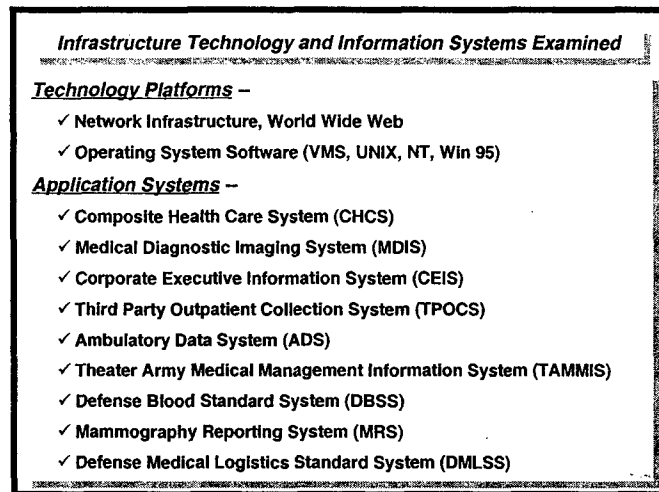
In the **Technology Reviews**, machine- and operating system-specific scripts provided by the DHIAP team were executed (in cooperation with the MTF system administrators) to collect information about the configuration and characteristics of each targeted system. Each review was tailored to the specific application and to the specific computer's operating system and other technical characteristics.

Information collected in the Technology Reviews and Interviews included system type and status, software packages and patches installed, configuration and services of the network, and configuration of the system itself. Results of the Reviews were analyzed by the DHIAP team, and significant observations became part of the final Technical Report later furnished to the site's Information Management Office.

**ISE ACTIVITIES: (3) Wrap-Up and Reporting**

**Data Analysis.** The team analyzed and correlated all information gathered during the preceding ISE activities and documented their observations regarding the state of information assurance at the MTF at the time of the ISE. Then, applying knowledge of currently accepted practices for protecting information and of methods for securing information from threats known to be prevalent in the immediate future, they provided site-specific recommendations for MTF actions to improve the site's ability to protect sensitive information.

**Final Briefing and Technical Report.** Using the Observations and Recommendations compiled in the previous step, the DHIAP team prepared a presentation to summarize results of the ISE. They conducted a formal briefing for MTF leaders and appropriate staff, then conducted a more detailed briefing for the Information Management staff and others that had participated in the ISE interviews. Following these briefings, the team compiled the detailed technical findings that resulted from the External and Internal Probes, formulated recommendations for addressing areas of potential exposure, and provided this site-specific Technical Report to the site's Information Management Office.




**Figure A.4 – Technologies Examined**

The DHIAP Preliminary Survey was designed to gather an initial security/technical profile of sites that had chosen to apply for inclusion in DHIAP's ISE process. The full questionnaire used for Phase I ISEs is included below.

<b>Defense Healthcare Information Assurance Program (DHIAP) SURVEY</b>	
<b>Purpose</b>	
<p>This survey is designed to assist in selecting the DHIAP prototype sites. Sites selected will receive the advice and assistance of systems and security experts and implementation of a demonstration version of a secure health information system. Selection of the DHIAP demonstration site(s) will be based on the health information security profile developed as a result of this survey. DHIAP will demonstrate application of security policy, procedures, technology, and training to healthcare systems based on a requirement analysis by systems and security experts.</p> <p>This is NOT a command inspection. It is designed to be a quick survey of information security practices at your site. This information will be held in strict confidence and will only be used as part of the DHIAP.</p> <p>This questionnaire is designed for short answers that may be inserted in the response column. In some cases, additional explanation or documentation is requested in order to avoid lengthy questions. Request you forward the completed questionnaire with attachments to:</p> <p style="text-align: center;">MRMC-AT, Bldg 1054, Patchel Street Fort Detrick, Md. 21702-5012 Attn: DHIAP Team</p> <p>Electronic versions may be forwarded to <a href="mailto:security911@tatrc.org">security911@tatrc.org</a>. Questions regarding this survey may be directed to Mr. Willie Wright, TATRC, (301) 619-7034 or DSN 343-7034.</p>	
<b>QUESTION</b>	<b>RESPONSE</b>
0.0	<p>Has your organization performed a security risk assessment and/or accreditation of the medical information systems in the last 6 months. If so, please attach a copy of the findings and recommendations.</p>
<b>1.0 Organization</b>	
1.1	Provide the name, title and contact information of the organization's Chief Information Officer or Information System Administrator.
1.1.a	Describe his/her education and experience. Is the position full or part time? If part time what is the percentage of effort?
1.1.b	Describe his/her responsibilities. If part time state other responsibilities and percentage of effort.
1.1.c	Describe his/her reporting relationships (Chain of Command).
1.1.d	How long has this person held the position?
1.1.e	How long do you expect this person to remain in this position?
1.2	Provide the name, title and contact information of the organization's designated Systems Security Administrator or Chief Healthcare Information Security Officer.
1.2.a	Describe his/her education and experience. Is the position full or part time? If part time what is the percentage of effort?
1.2.b	Describe his/her responsibilities, authority and accountability. If part time state other responsibilities and percentage of effort.
1.2.c	Describe his/her reporting relationships (Chain of Command).
1.2.d	How long has this person held the position?
1.2.e	How long do you expect this person to remain in this position?
1.3	Provide the name, title and contact information of the individual who has authority to release patient identifiable electronic medical information
1.3.a	Describe his/her education and experience. Is the position full or part time? If part time what is the percentage of effort?
1.3.b	Describe his/her responsibilities, authority and accountability. If part time state other responsibilities and percentage of effort.

1.3.c	Describe his/her reporting relationships (Chain of Command).	
1.3.d	How long has this person held the position?	
1.3.e	How long do you expect this person to remain in this position?	
1.4	Provide an organizational chart of your IS and IS Security organizations.	
1.5	Have your organization done an AR 380-19 security checklist? If so, please attach.	
<b>2.0 Systems</b>		
2.1	List all relevant systems that contain patient identifiable data (CHCS and other clinical systems, CEIS and other administrative, business and finance systems, etc.).	
2.1.a	How many staff users per system?	
2.2	Are there other systems within your site with significant number of users or network impact? If so, please list and describe these systems to include number and type of users and network connectivity.	
2.3	Is your system administration centralized?	
2.4	List major applications used on PCs (e.g. Windows 95, Word, Excel, etc.)	
<b>3.0 Information Systems Security Policy</b>		
3.1	Is there a policy on release of personal identifiable confidential/private health information? If yes, please attach.	
3.2	Does your command have a documented IS security policy? If yes, please provide a copy of the document.	
3.2.a	How is the policy disseminated to your military staff, civilian employees, and contractors.	
3.2.b	How do you document acknowledgement and understanding of the instructions?	
3.3	Does the site have a documented role based access control policy? If yes, please provide a copy of the document.	
3.4	How do you exercise configuration control for software / hardware modifications and upgrades?	
3.5	Is there a process for introducing new equipment (such as hosts, printers, or modems)?	
3.6	Who (by position) is authorized to install hardware devices (modems, printers, disk drives, etc.) on personal workstations?	
3.7	Do users install software and/or hardware on their systems?	
3.8	Do you have a policy regarding the installation of unauthorized, copyrighted software on the system? Describe (or attach policy documents).	
3.8.a	How is the policy enforced?	
3.8.b	How do you detect violations of the policy.	
3.9	Describe your password management policy (for example, one-time passwords, password aging, and password quality) or attach policy.	
3.10	Describe procedures for removal of accounts/access for terminating/transferring users or attached policy.	
<b>4.0 Security Implementation</b>		
4.1	Describe the process of educating staff and employees regarding security policy/plans/practices	
4.2	Describe your security intrusion/attack response plan.	
4.3	What security tools (for example wrappers, COPS, tripwire) are used for system administration?	
4.4	Do employees use virus scanners?	
4.5	What methods are used to audit your systems and your networks?	

4.6	How do you assure that all systems are up-to-date with respect to known security patches, ACERT, etc.?	
4.7	What authentication mechanisms (e.g., standard passwords, one-time passwords, Smartcards, Biometrics, fortezza) are used and where?	
4.8	Are any inactivity log-off mechanisms used? What type and where?	
<b>5.0 Security Violations</b>		
5.1	Do you have procedures for reporting a suspected security violation? If yes, attach.	
5.2	Could it be determined if there was a break-in to one of your systems? If yes, describe the process or attach documents.	
5.3	Could it be determined if your firewall is functioning correctly? If yes, attach the relevant descriptions of the process or attach documents.	
<b>6.0 Network</b>		
6.1	If you had a network problem, who would you call?	
6.2	How many workstations are supported by the network(s)? How many are smart terminals and how many dumb terminals?	
6.3	Provide a chart or description of networks at your site.	
6.4	What tools are used for network administration?	
6.5	Provide a copy of your disaster recovery plan or COOP.	
6.6	What external network system does your organization connect to?	
6.6.a	How do you make sure you can locate them?	
6.6.b	Can employees configure modems for dial-in?	
6.7	Who (by position) is authorized to install hardware devices (modems, printers, disk drives, etc.) on your networks?	
<b>7.0 External Connectivity</b>		
7.1	Do you have explicit policies regarding the use of the WWW, ftp, telnet, video, and modem connectivity? If so, please attach documents.	
7.2	Do your patients and their caregivers exchange information via email or the internet?	
7.3	Do you allow access to your systems from the outside? If yes, who?	
7.3.a	What technologies are used for such access?	
7.3.b	What services to the outside do you provide with such access?	
7.3.c	If you provide web or ftp services to the internet, what steps do you take to protect the content on your web and/or ftp servers?	
<b>8.0 Vendor Services</b>		
8.1	Are vendors authorized to maintain your networks (i.e., routers, systems, and applications)?	
8.1.a	Is advanced notice required concerning changes?	
8.1.b	Do they have to explain how these changes will affect current systems, etc.?	
8.1.c	Is the maintenance done remotely?	
8.1.d	If so, what kind of access technology is used? (e.g., one-time passwords).	
8.1.e	Do vendors remove all vendor access passwords from your systems when they are no longer under contract?	
8.2	How do you validate vendor changes to your system?	
8.3	Do you provide access to your computing facilities to non-employees?	
8.3.a	Who and what are acceptable justification?	




*Defense Healthcare Information Assurance Program*



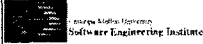

**An information assurance demonstration applied to Military Health Information Systems**

- Multi-year, multi-phase program designed to:
  - Further understanding of vulnerabilities inherent in health information systems of the MHS
  - Demonstrate feasible IS protection approaches
  - Research emerging information security technologies


**Slide 1**



*Team Members*

	<b>Advanced Technology Institute</b> lead in NIST ATP for Healthcare Information Infrastructure Technology
	<b>Lockheed Martin Energy Systems</b> prime for DOE's Oakridge National Laboratory
	<b>Software Engineering Institute</b> CERT Coordination Center
	<b>Healthcare Open System &amp; Trials</b> Healthcare Information systems consortium


**Slide 2**



*Program Description*

- Phase I
  - Evaluate information system security at designated healthcare sites
  - Design and develop secure system prototype to address identified vulnerabilities
  - Demonstrate secured systems operations
  - Evaluate results and capture lessons learned
- Phase II
  - Apply methodology to additional sites
  - Apply methodology to additional systems


**Slide 3**



*Information Security Evaluation*

- Address policy, procedures, technology, organizational, and programmatic issues
- Requires site cooperation and investment
- Includes technical review and staff interviews
- Generates site-specific vulnerability assessment
  - indicator of information system security across Military Health System


**Slide 4**



*Demonstration System Design*

- Select system to secure based on site evaluation
- Challenge is to partition a "segment from the whole" health information system
- Design will include policy and procedure recommendations as well as technology


**Slide 5**



*Demonstrate Systems Operation*

- Install and operate secured system to address operational realities
- Train staff, managers, and users
- Objective: leave behind a tangible operational system improvement


**Slide 6**



*Evaluate and Lessons Learned*

- Evaluation and lessons learned - an ongoing process
  - Evaluation team and evaluated site to assess effectiveness of evaluation methodology
  - SEI to evaluate ORNL design prior to installation and operation
  - Operation of demonstration evaluated by site, government, and team


Slide 7



*Information Security Evaluation Preview*

- Site Preparation Briefing
  - Support, Commitment, Understanding
- Site Data Collection
  - Site coordinator's role - key event
  - Potential probes to understand site configuration
- Data Analysis - Tailor approach to site
- On-site Visit
- Post Visit Data Review and Synthesis
- Results Briefing


Slide 8



*Site Evaluation Milestones*

ID	Task Name	Duration	Month 1			Month 2			Month 3						
			W-1	W1	W2	W1	W2	W3	W4	W1	W2	W3			
1	Site Evaluation	49 days													
2	Site Briefing	1 day													
3	Site Data Collection	10 days													
4	Team Preparation	6 days													
5	Team's Pre-briefing preparation	2 days													
6	Pre-technology review preparation	2 days													
7	On-site Data Collection	2 days													
8	on-site preparation	1 day													
9	on-site technology review	1 day													
10	Data Analysis	6 days													
11	post-incident data analysis	2 days													
12	post-technology review data analysis	2 days													
13	briefing worksheets and preparation	4 days													
14	Feedback	1 day													
15	Team de-briefing	1 day													
16	final briefing	1 day													
17	Evaluate methodology and review	1 day													


Slide 9



*Following ISE*

- System Selection
- Secure Solutions Design
- Demonstration
- Operation for Validation
- Transition to Site

Slide 10



*Follow-on Phases*

- Profile vulnerability for military healthcare sites by evaluating additional sites
- Demonstrate scalability of technology by implementing secured system at multiple sites
- Demonstrate applicability of methodology by repeating evaluation / design / demonstrate process on additional systems

Slide 11

A preliminary design review was held with TATRC, Eisenhower Army Medical Center and Winn Army Community Hospital. The report of that review to include significant issues developed by the participants and the presentation material used during the course of those meetings are attached as appendices B-1 and B-2 respectively.





**Contract No: DAMD17-99-C-9001**

Defense Healthcare Information Assurance Program (DHIAP)

Medical Treatment Facilities (MTF) Preliminary Design Review

August 26, 1999

Prepared for:

U.S. Army Medical Research and Material Command

Fort Detrick

Frederick, MD 21702-5012

Principal Investigator: Archie Andrews

843-760-4537

Advanced Technology Institute

5300 International Blvd.

N. Charleston, SC 29418

**Table of Contents**

<b>1. BACKGROUND</b>	<b>33</b>
<b>2. PURPOSE</b>	<b>33</b>
<b>3. RADIUS BACKGROUND</b>	<b>34</b>
Client/Server Model	34
Network Security	34
Flexible Authentication Mechanisms	34
<b>4. HIGHLIGHTS: PRELIMINARY DESIGN REVIEW WITH DDEAMC</b>	<b>34</b>
<b>5. HIGHLIGHTS OF PRELIMINARY DESIGN REVIEW WITH WACH</b>	<b>36</b>
<b>6. PLANNED ACTIVITIES</b>	<b>37</b>
<b>ATTACHMENTS</b>	<b>37</b>

## **1. Background**

The objective of the Defense Healthcare Information Assurance Program (DHIAP) is to ensure that clinical and other health related data of Department of Defense active duty personnel and other beneficiary populations are readily accessible but only as authorized. The DHIAP program will:

- Evaluate installed medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities,
- Validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems,
- Implement security solutions for evaluation within the military-civilian medical community.

The evaluation phase identified areas for demonstration of technological improvements. The DHIAP Team began detailed research for a demonstration system based on operational needs identified as a result of the Information Security Evaluations (ISE). The target area selected for the demonstration focus was remote access. The DHIAP team met with key network administrators and managers at Dwight David Eisenhower Army Medical Center (DDEAMC) to obtain detailed logical and physical descriptions of the DDEAMC and the Southeast Region Medical Command (SERMC) network. These meetings included discussions on critical needs at DDEAMC. DDEAMC identified the need for a remote access server that would comply with Department of the Army directives. The specific target technology selected in conjunction with the Medical Treatment Facility (MTF) test bed sites was a RADIUS (Remote Access Dial In User System) compliant server system designed to aid in identification and authentication of dial in users and comply with Department of Army guidance.

## **2. Purpose**

The purpose of preliminary design review for the MTF test bed sites was to get the site's input on the proposed technical and operational approach, to review the technical design of the proposal, and to gather site comments on operational requirements to include in the demonstration phase.

The application and installation of a remote access server that is RADIUS compliant was reviewed. An architecture and methodology was discussed and a methodology and schedule were agreed. That schedule was used as input to the Phase I schedule. The plan is to target the DDEAMC network for initial installation and testing while building a generic capability. The generalization of the installation and operation will be demonstrated by implementing a similar demonstration capability at Winn Army Community Hospital (WACH). Operational

issues of single site operation and remote access service in a regional environment will be explored.

### **3. Radius Background**

The following information was adapted from a report by Cisco Corporation comparing Lucent developed RADIUS protocol with Cisco developed TACAS+ protocol.

RADIUS is an access server authentication, authorization, and accounting protocol originally developed by Livingston Enterprises, Inc. (Livingston Enterprises is now part of Lucent). It is a system of distributed security that secures remote access to networks and network services against unauthorized access. RADIUS is comprised of three components:

- a protocol with a frame format that utilizes UDP/IP
- a server
- a client

The server runs on a central computer typically at the customer's site, while the clients reside in the dial-up access servers and can be distributed throughout the network.

#### **Client/Server Model**

A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. The RADIUS servers can act as proxy clients to other kinds of authentication servers.

#### **Network Security**

Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecured network could determine a user's password.

#### **Flexible Authentication Mechanisms**

The RADIUS server supports a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP PAP or CHAP, UNIX login, and other authentication mechanisms.

### **4. Highlights: Preliminary Design Review with DDEAMC**

On August 18, 1999, a video teleconference was conducted between ATI, TATRC, and DDEAMC to review the preliminary system design and obtain acceptance from DDEAMC and TATRC on the technical approach. The design of the RADIUS compliant dial-up solution for DDEAMC was performed by LMES DSRD at Oak Ridge National Laboratory.

The slides used for the Preliminary Design Review are contained in Attachment 1.

Key points from the design review are outlined below:

- TATRC reiterated to DDEAMC that this design was to be at no cost to DDEAMC except for their resources to maintain the system. DDEAMC asked if additional resources would be required to manage the system after it was installed. LMES responded that the goal is to keep the net resource additions at DDEAMC to zero, but the system would have to be demonstrated and evaluated before they could be sure.
- DDEAMC stated that they require a rack for the equipment to be installed at their site.
- The system requirements, previously agreed to on July 13 & 14, 1999 at DDEAMC, were reviewed.
- It was agreed to provide an initial capability for 24 dial-ins. This is a slight increase over the current number but will provide adequate capability for present needs and some early growth. DDEAMC wants the system to be scalable in the future so they can grow with the potential demand, but currently they estimate that 24 will be more than enough. Lines are already in and ready for use.
- LMES reviewed the alternative systems studied for this implementation. The CiscoSecure 3640 system by CISCO Systems was recommended for the following reasons:
  - Ease of maintenance
  - Supports remote management
  - Can authenticate against the Windows Domain Name/Password Database
  - Supports third party token-card servers
  - Logging and auditing are supported
- A diagram of the design is contained in the slides from the DDEAMC VTC (Attachment 1).
- DDEAMC stated the need to start off at 10BaseT for their network connection with the ability to progress up to 100BaseT.
- Support is not a significant issue, as DDEAMC will have approximately ten months left of contracted maintenance support after they receive the equipment. During that time they will incorporate support requirements into their existing support agreements.
- TATRC proposed that this prototype solution should serve both test sites (DDEAMC and WACH) and serve as a model for the entire region.
- Policy revisions to support the dial in capability were discussed and it was agreed that LMES will provide a draft appendix to DDEAMC Security Guidance, DDEAMC Regulation 380-3 currently under revision, to document recommended procedure for dial in to DDEAMC. DDEAMC will send an early draft of the Regulation 380-3 to LMES. LMES will review and make recommendations for possible policy guidance changes regarding dial-in use.

- Equipment will be Y2K compliant except for the Microsoft NT server. The NT server is pending revision by Microsoft, DDEAMC is aware of the status and is currently dealing with the same issue on all of their other NT devices. This caveat was understood by and acceptable to DDEAMC.
- DDEAMC requested clarification on how they were to fund their temporary duty (TDY) to view the demonstration, initially planned for Oak Ridge National Laboratory. DHIAP agreed to resolve that issue prior to 30 August.

## **5. Highlights of Preliminary Design Review with WACH**

On 19 August, the DHIAP design team visited Winn Army Community Hospital at Ft. Stewart, GA in order to bring them up to date on the intended demonstration system and to incorporate their requirements into the operational test plan. The design proposed for WACH was identical to that proposed for DDEAMC. The intent is to use the demonstration and testing phase to address operational alternatives that may affect hardware configuration decisions.

The slides used for the Preliminary Design Review at WACH are contained in Attachment 2.

Key points from the design review are as follows:

- WACH would prefer that DDEAMC run a centralized Remote Access Server to provide the identification and authentication system. This requirement elicited much discussion about the operational impact to WACH and DDEAMC and the rest of the region. It was agreed that the role for the DHIAP program was to provide expert advice based on a thorough understanding of the operational ramifications of alternative operational architectures. DHIAP will plan a joint meeting during the demonstration to help facilitate resolution of operational issues. Factors to be considered and addressed include options for configuration of permissions for the RADIUS clients, alternatives for managing identification and authentication, i.e., completely autonomous, distributed with backup or fully centralized.
- WACH had a concern over the potential cost of long distance service for subscribers that are remote. It was suggested that DDEAMC provide a centralized 800 service for the region along with the centralized I&A function.
- WACH stated that six modems are dedicated currently for continuous off-site connections. Presently other users dial in via the Director of Information Management (DOIM) facility.
- MEDCOM presently provides all Cisco router support for WACH. That support agreement will have to be modified to include any additional equipment.
- The point was made that the systems administrators at WACH wanted to ability and the knowledge to manage the system in an emergency whether it was centrally administered or not.

- WACH agreed with the system requirements, pending resolution of the operational issues involved with centralized or distributed management of the remote access server capability. They also agreed that resolution of that issue could await the demonstration.
- WACH also wanted to know if funds were available to fund their travel to the demonstration. Clarification was promised by August 30, 1999.

**6. Planned Activities**

Based on the stated requirements for analysis of both an autonomous Remote Access Server (RAS) and a centralized facility, the DHIAP team plans to proceed as follows:

- Plan on a multi-site demonstration in order to analyze the operational impact of the various alternatives (permission option configurations, centralized versus decentralized operations, etc.).
- Proceed with earliest installation at Oak Ridge National Laboratory but plan on incremental add to demonstration of sites at ATI and TATRC. ATI to add first in order to sort out test parameters for multiple sites and TATRC to follow to assess 3 site operations as model for region.
- Demonstrate operations in Charleston in order to minimize TDY costs and to maximize ability of sites to view, participate and assess results.
- The demonstration and testing along with the operational review will define the baseline set of equipment for installation at the sites. This equipment will be acquired as soon as practical after confirmation of the most desirable configuration.

DHIAP has identified the following immediate actions:

<b>Action:</b>	<b>Dependency:</b>
Ordering equipment for LMES	Approval from Contracting Officer
Ordering equipment for ATI	Approval from Contracting Officer
Ordering equipment for TATRC	Approval from Contracting Officer
Ordering equipment for DDEAMC & WACH	Identification of baseline equipment configuration; Demonstration and resolution of operational issues that may affect equipment set.

In addition to the equipment acquisition, demonstration and installation, the DHIAP team will produce a template for remote access procedure for the use of dial in.

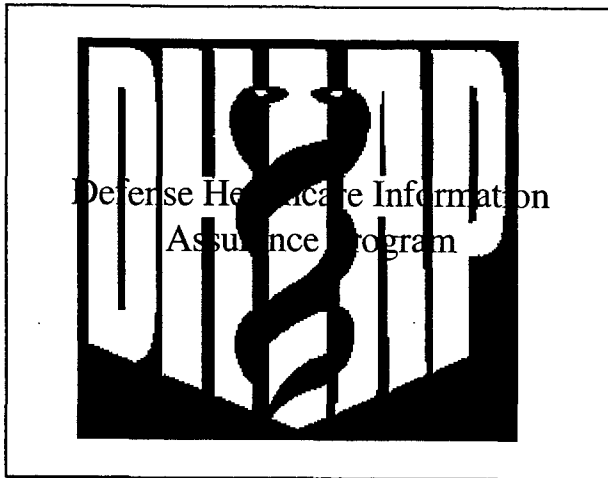
**Attachments**

- Attachment 1: Presentation for DDEAMC VTC Design Review [see **DHIAP Annual Report Appendix B-2 for the presentation used with both sites**]
- Attachment 2: Presentation for WACH On-Site Design Review [see **DHIAP Annual Report Appendix B-2 for the presentation used with both sites**]
- Attachment 3: Equipment List for Demonstration prototype [included on this page]

**Attachment 3:  
Baseline Equipment List for Demonstrations at LMES, ATI, TATRC,  
DDEAMC, WACH**

<b>Main Router</b>			
<b>Item</b>	<b>Part No.</b>	<b>Description</b>	<b>Notes</b>
3640 Chasis	CISCO3640	3600 4-slot Modular Router-AC with IP software	
Power Cord	CAB-AC	Power Cord, 110V	
Operating Software	S364CP-12.0.4T	IP Plus	
Flash Upgrade	MEM3600-8U16FS	8-to-16MB Flach Factory Upgrade for the Cisco 3600	
Enet Poet	NM-1FE-TX	1 port Fast Ethernet Network Module (TX only)	The port is a 10/100 port
8 Port modem	NM-8AM	8 port Analog Modem Network Module	
16 Port modem	NM-16AM	16 port Analog Modem Network Module	
Support	CON-SNT-3640	Cisco 3640 SMARTnet Maintenance	
<b>RADIUS Server</b>			
<b>Item</b>	<b>Part No.</b>	<b>Description</b>	
RADUIUS SW	CSNT-2.3	CiscoSecure ACS V2,3 for NT	
Support	CON-SAU-CSNT	SAU Service, CiscoSecure for NT	
Server		Pentium III, 450 MHz, 512 Cache, 128 M Ram, 10G HD, 32x CD-ROM, 12 G Tape Backup, 10/100 TX UTP NIC, hi res video card	
Monitor		17" High Res	
OS		NT Server 4.x	
Network cables			





**Slide 1**

**DHIAP AGENDA**  
**RADIUS Prototype Discussion**  
**1100 August 19, 1999**

- Introductions 10
- Re-Statement of DHIAP intent - Arch 10
- Summary of DHIAP Progress to date - Arch 10
- Prototype Development Schedule - Steve 10
- RADIUS prototype discussion - Forrest 30
- Comments on prototype - WACH 20
- Associated Policy - Steve 10
- Wrap up - Arch 10

**Slide 2**

- DHIAP Objectives**
- Ensure that patient clinical and other health related data is readily accessible but only to authorized healthcare workers.
- Evaluate existing medical information systems to determine vulnerabilities and recommend operational policy and procedures to address
  - Propose and validate technical solutions that assist in ensuring the integrity and security of data in medical information systems
  - Provide technical and programmatic advice regarding long range programs to address information assurance
  - Provide authorized users appropriate access to data resources from non-secure environments
  - Implement the systems for evaluation

**Slide 3**

- Areas of work**
- Technical Assessments
  - Prototype Development
  - Prototype Demonstration
  - Technology Transfer

**Slide 4**

- Progress to Date**
- Technical Assessments of test bed sites completed - May
  - Demonstration area - remote access - agreed - May
  - Target - RADIUS compliant server - selected - July
  - Schedule proposed and agreed - July
  - Requirements developed and refined - July
  - Baseline equipment set proposed - August

**Slide 5**

- Purpose of this Meeting**
- Understand and buy-in to technical approach
  - Verify that operational requirements are likely to be satisfied
  - Identify operational interests of particular concern to be addressed in test and demonstration phase
  - Update projected schedule
  - Answer questions and identify unresolved issues

**Slide 6**

**DEMO SCHEDULE**

• Preliminary Design	D+10
• Understand configuration	D+15
• Equipment List	design + 10
• Acquire equipment	list + 15
• Install equipment in Oak Ridge	acquire + 10
• Demonstrate in Oak Ridge	install + 20
• Install at site #1	demo + 30
• Test at site #1	install + 10
• Demo & train at site #1	test + 10
• Demo & Train at site #2	site #1 + 30

**REQUIREMENTS**

1. RADIUS compliant (SAIS-IAS msg, 231300Z APR 99)
2. Rack mounted (router and RAS)
3. Compatible with existing hardware/software resources
4. Minimize administration/support burden
5. 16 discrete, dial-in, voice grade POTS lines
6. Remote management

**Slide 7**

**DERIVED REQUIREMENTS**

1. ID, Authentication and Authorization for user
2. Accounting information (who and when)
3. CISCO and NT, if reasonable
4. Growth in number of lines and types of connections
5. Options for other technologies (tokens, smart cards, etc)
6. Single vendor solution, if reasonable

**Slide 8**

**ALTERNATIVES REVIEWED**

1. VOP Radius Server by Viroom Products
  - Not NT or CISCO - limited growth for Phase 2
2. Total Control Access Platform, by 3COM
  - Limited features - limited growth.
3. Remote Authentication Dial-In User Services by Bay Networks
  - Unstable Product Line (Nortel just bought Bay)
  - Does not work with CISCO
4. CiscoSecure by CISCO Systems.
  - Later Slide
5. Mini/ArrayIII by MultiTech Systems.
  - Limited Products, limited growth
6. PortMaster by Lucent Technologies.
  - High Cost, not CISCO compatible
7. Microsoft RAS
  - Limited connections and growth

**Slide 9**

**CiscoSecure for Windows NT**

Has a built-in web server for support using an HTML interface

- Supports remote management and common user interface

Can authenticate against the Windows Domain Name/Password Database

- Reduce user burden

Supports third-party token-card servers (SecurID, Enigma Logic, SecureNet, and any hexadecimal X.909)

- Growth into Phase II

TACACS and RADIUS supported - Both can run at the same time


Logging and auditing supported

**Slide 10**

**CISCO 3640 ROUTER**

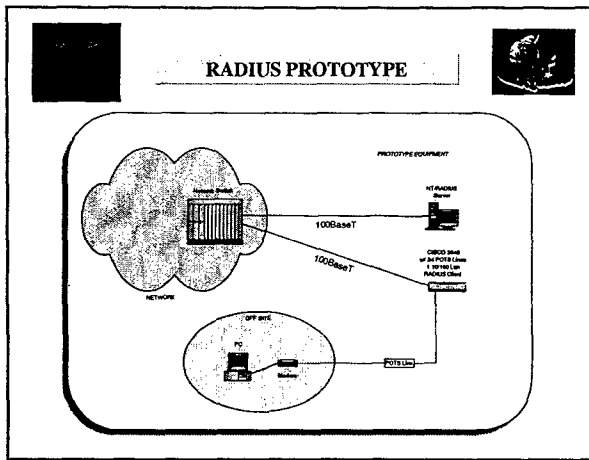
**CISCO 3640 Access Concentrator**

- 24 Analog Modem Ports (16 and 8)
- 10/100 Ethernet port
- CISCOSecure Client
- IPSec 3DES
- Growth through modules



**Slide 11**

**Slide 12**



Slide 13

**LOCAL OR REGIONAL**

1. CISCO routers common throughout region
2. NT becoming the region standard OS
3. CiscoSecure supports replication and a hierarchy for I&A
  - Research area for shared lists and management of database

Slide 14

**SCHEDULE**  
continued

- Review existing guidance on remote access
- Develop equipment specific procedure guides if needed following installation in Oak Ridge demo + 10

Slide 15

**RADIUS POLICY and PROCEDURES**

Develop recommendations for dial-in procedure as MTF deems appropriate

Policy modification recommendations as appropriate

Slide 16

**POLICY**

Potential Policy Issues

- Remote Dial-up usage
- Password management
- Network access
- Configuration management (modems)

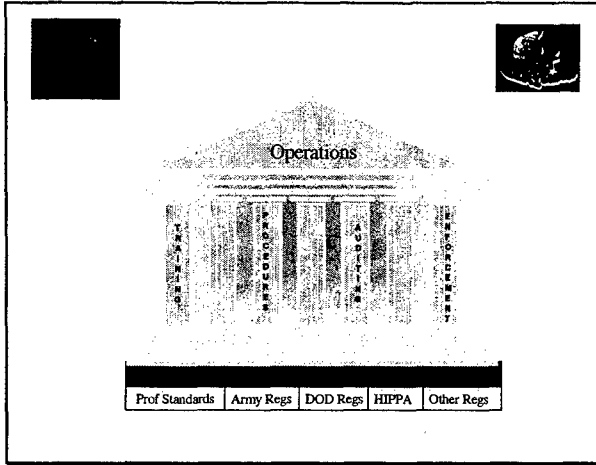
Slide 17

**PROCEDURE**

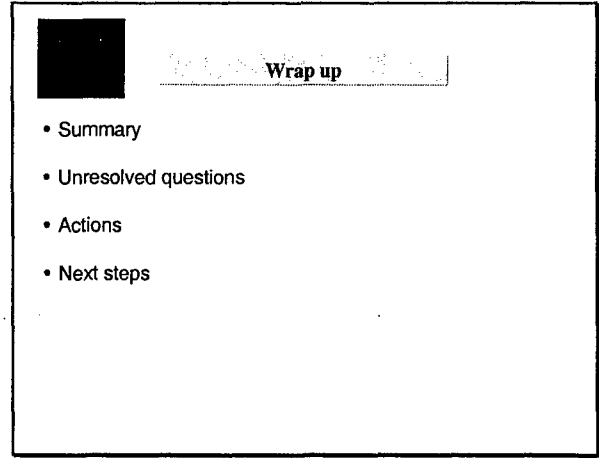
Potential Procedure Issues

- User
  - Obtain phone number, UID & password
  - Dial
  - Authenticate
- Administrator
  - Enter valid users
  - Assign passwords
- ISSO
  - Review usage logs

Slide 18



**Slide 19**



**Slide 20**

The demonstration program is designed to address one area of technology. Other areas of technology that are emerging or that have potential for high impact on the MTF were considered and research areas proposed. White papers proposing research on subjects relevant to the MTF Information Security were proposed and research reports are in progress. The white papers proposing the research are attached as Appendices C-1 through C-3.

## **Public Key Infrastructure**

**Problem:** How do youPublic Key Infrastructure provides a facility to encrypt and thereby protect the integrity and confidentiality of sensitive documents as well as providing a facility for a non-reputable electronic signature. DOD has announced a strategic direction to take advantage of this capability but the implications of implementing and applying PKI is not well understood. This research will focus on understanding the implications of implementing a public key infrastructure (PKI) in a military medical treatment facility (MTF) environment.

**Hypothesis:** Implementing a PKI in a military MTF environment will substantially increase information integrity, availability, confidentiality, and non-repudiation without substantially increasing the burden on the information management staff. The use of public key encryption to secure electronic commerce will increase, and interactions with healthcare benefit providers will require its use. A PKI implementation that provides interoperability and cross certification capabilities across various enterprises will be necessary. Integration of PKI into existing applications will be required.

**Research Objective:** This paper research will examine the implications of implementing a PKI in a military MTF environment. It will define the components of a typical PKI and the security requirements for those components. It will address current implementations in both the government and private industry and define any issues peculiar to the military MTF environment. It will address potential implementation schemes for PKI and propose possible alternative approaches to address areas where PKI is not appropriate.

### **Methodology:**

1. The research team will investigate current and emerging PKI tools and techniques to determine the burden they might impose on a military MTF and compare this with the number and skills of the information management staff at an MTF. This will include (but not be limited to) a review of the recently announced DOD pilot PKI program, based on Netscape's Certificate Management System 4.1.
2. The research team will base their investigation on a typical MTF(s) to ascertain application of PKI to information systems currently in use, practical use of electronic signature with current procedures, the potential benefit of using PKI to increase information assurance (information integrity, availability, confidentiality, and non-repudiation) among those systems and in external communications with healthcare providers, and the resources required to implement PKI in the military MTF domain.
3. Where existing and emerging PKI tools and techniques fall short of MTF needs or create a seemingly unacceptable burden, the research team will consider alternative methods to various aspects of those tools and techniques. The team will attempt to assess the pros and cons of those alternatives.

**Expected Results:** The research team expects to find that some PKI tools and techniques are appropriate for MTFs and that there is some increased burden on the information management staff in implementing those PKIs.

**Anticipated Product:** The research team anticipates producing a comprehensive report on the state of PKIs and the needs of MTFs for such techniques. This report will include recommendations for consideration by those MTFs and by the DOD medical community in general.

**Schedule:** This report is estimated to require 6 man weeks for research and writing over a four month period.

**Qualifications of the Investigator:** The principle investigator has over thirty-five years in information security with emphasis on encryption tools and techniques. He has implemented (and developed implementation plans) such tools throughout the federal government. Recent work involved testing and evaluation of the infrastructure tools for the Defense Message System.

## **Trust-Model Development**

**Problem:** Current healthcare computer and network systems contain a number of vulnerabilities. One way to describe a system of vulnerabilities is through its opposite corollary, a system of "trust." This system of trust can be developed into a "trust-model" describing a computer and/or its associated network. A "trust-model" describes who the system will allow in rather than who the system failed to keep out. This research will focus on understanding a trust-model sufficiently to evaluate its operational impact and implementation.

**Issue:** Healthcare systems contain "stovepipe" systems that are installed at the behest of others and are managed remotely. These systems are integrated into the hospital system. The result of integrating these systems is that they operate with a trust-model that allows complete trust between the stovepipe system and the hospital system. This model has a number of risks associated with it including:

- Monitoring of local network work traffic
  - User ids and passwords
  - Patient information
  - Email messages
  - System manager ids and passwords
  - Router traffic
- Attacks on local systems
  - Denial of service
  - Probing and exploitation of vulnerabilities
  - Masquerading as another host
- Gateway to other military sites.
- Mapping of the local network
- Email exploder site for Spam email
- FTP site
- HTTP site

In addition, local support personal are held "responsible" for the system and its impact on the overall system without the authority to act in the hospital's best interest.

When looking at the possible trust-model solutions, it is important that they be constrained by the necessity to implement a solution without adversely impacting operations.

**Research Objective:** The objective of this research is to describe how to develop a "trust-model" for a network. The research to be performed will look at many different areas including network configurations, router configurations and firewall implementation. It is anticipated that there will be multiple possible solutions providing complete and incomplete coverage of possible security risks. Each solution may consist of implementing multiple actions to provide the certain level of security with an associated level of risk and effort.

In addition to increasing the security of the local hospital network, the objectives are to:



- Determine the impact and limitations of various solutions;
- Maintain application usability and operation;
- Maintain client connectivity to the host; and
- Continue to allow remote system administration of the host.

**Methodology:** The areas that will be examined include network configurations to determine the impact of using network switches and virtual LANS. Other areas include the examination of various router configurations to determine the impact of IP address filtering, protocol filtering, port filtering, and initiation filtering. The installation of firewalls and their configurations will also be examined. This will be an examination of the current literature and implementation guidance for network configurations and hosts. It will describe and discuss architectural alternatives.

**Expected Results:** A description of generalized architectural alternatives in the form of templates that can be applied based on the level of effort, network impact, cost and risk.

**Anticipated Product:** The product of this research will be a paper describing each template with its associated level-of-effort, network impact, cost and risk

**Schedule:** It is estimated that this research will take six weeks of effort over a time period of three months.

**Qualifications of Investigator:** Dr. Jack Stinson will be the primary investigator. Dr. Stinson is a Principal Engineer at the Advanced Technology Institute (ATI) with over twenty-five years of industrial and academic engineering experience. He is a key technical resource on the DHIAP program and has been a team member of the two Information Security Evaluations (ISEs) that have been performed on Army Medical Hospitals. In addition, he is the Program Manager for the Rapid-Prototyping of Application Specific Signal Processors (RASSP) Education and Facilitation (E&F) program which is ending. Dr. Stinson is also the Technical Manager for ATI's Computer Development Lab, which consists of diverse computers and operating systems. Dr. Stinson is proficient in several high level computer languages, assembly languages, and simulation languages. He has worked extensively with UNIX computer systems and computer networking and was responsible for establishing the Internet connection at ATI.

Prior to joining ATI, Dr. Stinson served as Associate Professor of Electrical Engineering at The Citadel for sixteen years. He taught courses in electronics, communications, digital logic, computer programming, microprocessor architecture, and circuits. He was also a member of a research team that provided the National Security Agency with background information on the more technical aspects of database systems and local area network response problems.

Dr. Stinson is a registered Professional Engineer in the state of South Carolina, a member of Tau Beta Pi engineering honor society and a senior member of the IEEE.

## **Remote Administration**

**Problem:** How do you balance the economy of remote central administration of standard information systems with a site's responsibility for the security of its systems? Military medical treatment facilities (MTFs) operate about a dozen "standard" information systems developed by higher echelon agencies and frequently administered by those agencies or their surrogates. At best, that remote administration represents a very large unknown to the local information system security officer (ISSO). At worst, it represents an easily compromised conduit to that remotely administered system and every other system on the MTF's network. Because the remote administration is performed by or contracted by a higher headquarters (Army Medical Command, OSD/Health Affairs, Regional MTF or Program Manager for CHCS), the MTF often has no knowledge of the identity or location of the administrator and no influence over the tools and techniques used by that administrator.

**Hypothesis:** If the MTF has effective policy, management support, and effective monitoring tools; then the potential risks created by remote administration will be reduced and visible enough to manage.

**Research Objective:** This research will accomplish two main objectives: define the problem in terms of actual practices, inter-agency relationships, and existing policies, and discuss potential changes in policies and practices to improve MTF control of external administrators, minimize exposure of administrators' traffic, and reduce exposure of other local systems should the remotely administered system be compromised.

**Methodology:** The research team will

1. Begin by reviewing the results of the DHIAP ISEs. Those results included several instances of remote system administration. Emphasis will be on MTF information security policies, controls the MTFs exercise over external administrators, isolation of externally administered systems, and plans for the future.
2. Interview the administrators / program managers of those systems that operate within MTFs' networks and are administered from an external location. The objective of these interviews will be to ascertain the information assurance measures the administrators observe and to better understand their motivations, constraints, policies, and plans for the future.
3. Investigate existing and emerging technology for protected remote access, for monitoring administrators' activities, and for system isolation.
4. Investigate modification of MTF and higher echelon policies to meet the missions of both with minimum exposure of sensitive information and systems processing that information.

**Expected Results:** The research team expects to find that:

1. MTF policies do not adequately address remote access and that remote administrators would comply if adequate policies existed.
2. Remote administrators are motivated by economy of scale.

3. MTF computer networks can be segmented to minimize risk to other MTF systems.
4. Information protection measures observed by remote administrators span the spectrum from open transmission telnet or root (single user) passwords to end-to-end protected sessions using one-time passwords while MTF administrators capture a complete audit trail of all keystrokes.
5. Better practices and tools can be incorporated by the remote administrators who currently use less effective measures.
6. Some new tools and techniques can be developed and incorporated to support all parties' objectives.

**Anticipated Product:** The research team anticipates producing a comprehensive report on the state of remote administration and the risks it currently presents to information assurance at MTFs. This report will include recommendations for consideration by those MTFs and by the DOD medical community in general for maintaining the economy of scale offered by remote administration while providing the MTF ISSO an acceptable level of information protection.

**Schedule:** This report will be released to the Advanced Technology Institute no later than November 1999.

**Qualifications of the Investigators:** The principle investigator has over thirty years in military information system design, development, operation, and administration, including system security, management of subordinate sites, and interaction with higher echelon system managers. Over the past three years, his focus has been on patient confidentiality in the military medical arena.

**Annual Report**  
of the  
**Survivability Simulator Project<sup>†</sup>**  
October 1998 through September 1999

Work on the Survivability Simulator project this year includes theory, development and applications. Progress was made on the theory and formal characterization of survivability, unbounded systems, emergent algorithms and survivability architectures. Design of the EASEL simulation language and run-time environment continue on schedule. Several applications are being developed or studied for use of the simulator. Each of the above areas is discussed in more detail below.

### **Unbounded Systems**

An unbounded system is any system whose purpose or mission must be achieved in the absence of complete or precise information about some aspects of the system, in the absence of centralized administrative control, or in the presence of untrusted insiders. Examples would be the Internet, any system with distributed administrative control, any system with remote access, any system with unknown users, and any system containing COTS software. We refine the definition of unbounded system both formally and informally in [4]. Unbounded systems are critical to any discussion of Security because most traditional security technologies depend on a fortress model that requires closed systems with only trusted insiders, central administrative control, and complete knowledge of all system components. Almost all modern large scale systems are unbounded and thus cannot be protected by traditional security technologies that depend on a fortress model.

### **Survivability**

Survivability takes a different perspective on the problems that Security was intended to solve. We define survivability as the ability of a system to continue to fulfill its mission, in a timely manner, in the presence of attacks, failures, and accidents [1]. This year we continued to refine this concept from both technical [7] and business [8] perspectives. We are particularly concerned with survivability as it applies to critical national infrastructures not only because of their economic, political and social importance, but because broad-based infrastructures are inherently unbounded. Survivability also recognizes that the traditional security practices of emphasizing confidentiality over integrity and giving minimal concern to availability are inappropriate in modern large scale systems where availability of the systems services is often critical, integrity is usually very important, while confidentiality is less important.

Survivability views infrastructure assurance from a perspective of risk management applied to mission fulfillment in the context of unbounded systems. Work in this project focuses on establishing a scientific and mathematical base for survivability and in developing

---

<sup>†</sup> This work was performed at the Software Engineering Institute (SEI) and was sponsored in part by the U.S. Army Medical Research and Materiel Command under Contract No. DAMD17-99-C-9001 and by the U.S. Air Force Rome Laboratory AFRL/IFGB. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

techniques, tools, processes, and other technologies that support the development and operation of survivable systems.

### **Emergent Algorithms**

We define Emergent Algorithm (EA) informally as an efficient distributed computation that generates and preserves those global system-wide properties that constitute the mission requirements for a system. These global properties include both functional and nonfunctional properties and are called Emergent Properties because they typically emerge from the combined actions and interactions of the various components of a system and because they often do not, or cannot, prevail within individual components of the system. Emergent algorithm is defined more formally in [4]. Because we are interested in practical algorithms, we limit our consideration to emergent algorithms for which the resource costs (e.g., space, time, dollars) within each individual node are less than proportional to the total system size. Otherwise, as is the case with current IP routing on the Internet, the local costs (in storage for each router connected to the Internet) would grow at the same rate as the size of the system. This constraint is not only essential to practical solutions for large systems, but sufficiently constrains the development process that we have confidence in finding feasible solutions (or proving their non existence). For survivability, we also consider only algorithms in which there are no single, nor constant number of, points-of-failure. Although necessary for survivability, this latter restriction precludes all algorithms that depend on centralized control, hierarchical decomposition, centralized data, or nodes with unique rolls.

Early in the year we developed an emergent algorithm for Internet Routing [4]. Its primary purpose was to test our development methodology and to illustrate that practical emergent algorithms were possible. The resulting routing algorithm employs a source-routing method using standard IP addresses. Like conventional IP routing it has linear performance costs per node for routing, but unlike conventional IP routing it requires less than order  $n$  storage per node. This means that the storage space for an Internet router would drop from gigabytes to kilobytes. This routing algorithm is not yet practical because we have not yet developed the accompanying algorithm for dynamic updating of routing tables. This work should also be extended to include more survivability mechanisms within the algorithm and to address differing levels of trust that may exist within the network. Finally, certain aspects of the algorithm suggest that it may be applicable to dynamic connections in highly mobile systems without a need for fixed home sites.

### **Survivability Architecture**

Our work in unbounded systems, survivability, and emergent algorithms has led to a method for describing the architecture of survivability system in terms of the local actions of each type of participant in the system and the protocols of their interactions. This combination of local actions and neighbor interactions constitutes the critical aspects for survivability of a system and does not depend on knowledge of the specific topology or interconnections among individual components.

### **EASEL Language Design**

Most of the project effort this year has been on the language design and its implementation. The EASEL language has a simple generalized grammar [12] of the kind used in Algol,

Pascal, and Ada. The language directly supports the semantics of unbounded systems including independent specification of each actor or node within a system, concurrent execution semantics, multiple simultaneous neighbor definitions, protocols of neighbor interaction, and language enforced visibility restrictions consistent with the systems being described. Control and monitoring of the simulation is specified separately from the description of the system being simulated. Highlights of the language design are discussed in [6].

The language provides a property-based type (PBT) perspective on systems rather than an object-oriented view. This means that types are defined by their properties rather than by their representations, and that formally types are sets of properties rather than sets of objects conforming to those properties. Among other things, this accounts for and enables useful computation on distinct types for which there are no physical world examples. It means that the level of abstraction for a simulation can be varied by adding or removing properties from the descriptions, that types are first class entities that can be manipulated by programs, that valid simulations can be run with incomplete and imprecise descriptions, and that conclusions can be drawn about broad classes of examples as well as specific examples.

Types are typically defined as specializations of previously existing more general types. This specialization can be done by "and"ing existing types or by adding additional properties in the form of predicates or assertions. In all cases the new type automatically inherits all operations for every supertype of the existing type. Thus EASEL provides multiple inheritance of operations from arbitrarily many superclasses, with guaranteed consistency, and without explicit inheritance specifications. For example, all operations on real numbers and all operations on positive numbers are automatically defined for prime numbers because primes are simultaneously real numbers, positive, and integers.

Highly distributed computations are described in EASEL through formal specification of a survivability architecture. A program consists of descriptions of the actions of each participant in the system being simulated, of the neighbor relationships that exist, and of the protocols of interactions among neighbors. Additional facilitator and observer actors are defined to control and monitor the simulation process. Interactions between actors are defined within the affected actor's type definition where the affected actor is referred to by the pronoun "me" and the perpetrating actor is referred to as the pronoun "you". Not all types need be named. Anonymous types can be referred to by anding predicates to a known type, so that the predicate "integer & positive" can be used as an anaphoric reference to the type of all integers that are also positive.

The language supports a programming paradigm in which shared variables among concurrent processes and global visibility are neither necessary nor desirable. Independently developed simulations can coexist in a single program. By adding only the descriptions of their interactions, it is possible to simulate their interdependencies including for example cascade effects in infrastructure assurance applications. The author of a simulation may associate any amount of simulated time with any action or interaction within the simulation. This contrasts with most simulation languages which implement time as simulated delays at designated points in the program. The language's exception handling facility may be invoked by the system or by any application, but applies only to a single thread within the simulation. This is because once created actors have equal status with their parents and may outlive their

parents. There are a number of built-in types, operations, and neighbor relations that are of particular importance to survivability and security. These include communication neighbors, proximity neighbors, line-of-sight neighbors, and simulated mobile code. The built-in proximity and line-of-sight operations provide a two-dimensional toroidal space with arbitrary floating point positions in the range  $-2^{15}$  to  $2^{15}-1$  in each dimension.

### **Visualization System and User Interface**

The EASEL visualization system consists of user controlled windows that map to author specified views of the simulation. Simulations control the number of independent views and their content by specifying what, where, and at what scale depictions are to appear within each view. There are operations for constructing graphic depictions, but no drawing operations; drawing is implicit. The user running a simulation controls the number of windows, the size of each window, what view is associated with a given window, where the window is positioned within the view, and the magnification of the view within each window. There may be multiple windows per view and some views without windows. The interactive user interface provides user control of the simulation and its depictions through a system of menus and dialogs. User controls include the real time speed of the simulation, the granularity of the simulation time, and the ability of the user to act as a facilitator within the simulation by entering and executing arbitrary statements and expressions that will be interpreted within the context of the on-going simulator execution.

### **Pseudo Machine**

The target representation of EASEL programs consists of byte codes for a pseudo machine [6] analogous to Java byte codes. The byte codes provide an extremely space efficient representation of programs. The pseudo machine is stack oriented with single byte instructions for referencing and assigning variables, and for most commonly used Easel operations. Control and infrequently used operations are typically two bytes. The pseudo machine supports up to  $2^{15}$  bytes of code per segment, 256 routines per segment, 256 local variables per frame,  $2^{15}$  items per array or record, and  $2^{31}$  bytes per file. Most built-in Easel operations are one-to-one with the corresponding pseudo machine operations.

### **Simulator Implementation**

The simulator implementation consists of the author interface, translator, interpreter, run-time system, event processing, debugger, user interface and window system, visualization system, and input-output system [11]. The implementation of memory management and garbage collection are largely complete and substantial work has been done on the author interface (30%), translator (40%), event processing (80%), user interface (50%), window system (60%), visualization system (80%), and input-output system (60%). Work is just beginning on the interpreter and has not begun on the debugger. Although the total effort is substantial, the risk is largely one of engineering an appropriate combination of well known techniques or techniques familiar to the project leaders. Work on the various subsystems has been carefully coordinated so that integration and system-wide testing can be done after each incremental subsystem release. Typically, during times of intensive development (e.g. this past summer) when a large development was present (i.e., 10 students half to full time), there was a new system release five times per week. This ensures that each developer is aware of what the others are doing and does not make assumptions that would prevent proper integration. The

implementation work is being carried out in a development laboratory at the SEI established for the simulator project. Detailed descriptions of the methods, data representations, and algorithms for this years implementation effort are given in [13].

### **Applications**

Although it is too early to run real applications, several simple applications have been developed to test various aspects of the language design. One which simulates an ant undertaker and one that does neural net simulations have been particularly useful. The neural net application will also be helpful in testing the performance of the system. It is planned that it will be the first complete application to be run. It will be run before the simulator is complete by hand translating it to byte code and giving priority to the operations it uses in the implementation of the interpreter. It is particularly challenging because it will involve neural nets larger than those previously run in any simulation system. The ant undertaker application in addition to exercising a variety of the unique language features also includes dynamic graphic depictions that can be used to more thoroughly test the visualization and windowing systems.

Several masters students in the Information Network Institute (INI) at Carnegie Mellon University (CMU) are writing theses related to the simulator. Because the simulator will not be complete in the time frame of their theses, they are concentrating on identification of the mission requirements of particular infrastructures and on development of survivability architectures for those infrastructures. On-going thesis work is in health care infrastructure, electric power transmission, and financial transaction systems. Finally, on a low priority basis work is continuing on the development of an emergent algorithm for updating IP routing tables needed for our space efficient emergent routing algorithm. There has also been interest in using a modified emergent routing algorithm as an alternative to centralized Internet domain name (i.e. DNS) lookup.

### **Publications**

1. David A. Fisher and Howard F. Lipson, "Emergent Algorithms for Survivable Systems", Proceedings of the 1998 Information Survivability Workshop, October 28-30, Orlando, FL; Software Engineering Institute and IEEE Computer Society, 1998.
2. Tim Shimeall and David Fisher, "A Simulation Environment for Survivability Algorithms", Proceedings of the 1998 Information Survivability Workshop, October 28-30, Orlando, FL; Software Engineering Institute and IEEE Computer Society, 1998.
3. R. J. Ellison, D.A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, N. R. Mead, "A Survivable Network Analysis Method", Proceedings of the 1998 Information Survivability Workshop, October 28-30, Orlando, FL; Software Engineering Institute and IEEE Computer Society, 1998.
4. D. A. Fisher and H.F. Lipson, "Emergent Algorithms -- A New Method for Enhancing Survivability in Unbounded Systems", Proceedings of 32nd Annual Hawaii International Conference on System Sciences (HICSS-32), January 5-8, 1999, Maui, HI; IEEE CS Press, Los Alamitos, CA, 1999.



5. R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. A. Longstaff, N. R. Mead, "Survivable Systems: An Emerging Discipline", Proceedings of the 11th Canadian Information Technology Security Symposium (CITSS), May 10-14, 1999, Ottawa, Ontario, Communications Security Establishment, Government of Canada, 1999.
6. David A. Fisher, "Design and Implementation of EASEL -- A Language for Simulating Highly Distributed Systems", MacHack 14 the 14th Annual Conference for Leading Edge Developers, June 24-26, 1999, Dearborn, MI.
7. D. A. Fisher and H. F. Lipson, "Simulation and Visualization of Survivability Problems and Solutions", The 99 Software Engineering Symposium -- Improving the State of Software Engineering, August 30-Sept. 22, 1999, Pittsburgh, PA.
8. H.F. Lipson and D. A. Fisher, "Survivability -- A New Technical and Business Perspective on Security", New Security Paradigms Workshop 1999, September 21-24, Caledon Hills, ON; Association for Computing Machinery, New York, NY, 1999.
9. R.C. Linger, R. J. Ellison, D. A. Fisher, H.F. Lipson, T. A. Longstaff, N. R. Mead, "An Approach to Survivable Systems", NATO IST Symposium on Protecting Information Systems in the 21st Century; Washington, DC, October 25-27, 1999.
10. R. J. Ellison, D. A. Fisher, R.C. Linger, H.F. Lipson, T. A. Longstaff, N.R. Mead, "Survivability: Protecting Your Critical Systems", IEEE Internet Computing, November/December 1999.

**1. Background**

The objective of the Defense Healthcare Information Assurance Program (DHIAP) is to ensure that clinical and other health related data of Department of Defense active duty personnel and other beneficiary populations are readily accessible but only as authorized. The DHIAP program will:

- Evaluate installed medical information systems to determine vulnerabilities in information assurance capabilities and recommend operational procedures and policies to address those vulnerabilities,
- Validate proposed technical solutions and operations that ensure the integrity and security of clinical and other health-related data used and created in medical information systems,
- Implement security solutions for evaluation within the military-civilian medical community.

The evaluation phase identified areas for demonstration of technological improvements. The DHIAP Team began detailed research for a demonstration system based on operational needs identified as a result of the Information Security Evaluations (ISE). The target area selected for the demonstration focus was remote access. The DHIAP team met with key network administrators and managers at Dwight David Eisenhower Army Medical Center (DDEAMC) to obtain detailed logical and physical descriptions of the DDEAMC and the Southeast Region Medical Command (SERMC) network. These meetings included discussions on critical needs at DDEAMC. DDEAMC identified the need for a remote access server that would comply with Department of the Army directives. The specific target technology selected in conjunction with the Medical Treatment Facility (MTF) test bed sites was a RADIUS (Remote Access Dial In User System) compliant server system designed to aid in identification and authentication of dial in users and comply with Department of Army guidance.

The intention is to install configurations of the demonstration prototype, including equipment and software, at distributed sites to test the configuration options and the operational alternatives in order to demonstrate capabilities and make recommendations to the government. The demonstration sites will be located at Oak Ridge, Tennessee, Charleston, South Carolina, and Ft Detrick, Maryland.

**2. Operational Requirements**

The operational requirements of the demonstration and test should address the technical and operational areas in sufficient detail to provide an assessment of the available configuration alternatives and their operational impact when implementing a RADIUS compliant Remote Access Server capability for dial in users at the MTF.

The following operational requirements have been identified by the test bed sites and/or derived from the equipment characteristics:

- technical operations, i.e.:
  - normal user dial in:

- connect to CHCS emulation via a telnet session,
- connect to exchange server,
- restricted user dial in:
  - connect to router but restricted from exchange server access;
  - connect to router but restricted from CHCS access;
  - unauthorized user connect attempt;
- auditing of all user connect attempts and failures;
- graceful degradation in case of power failure via fail soft with "power-chute" UPS capability.
- subscriber configuration options for RADIUS, e.g.:
  - configuring the subscriber lines so connection is application specific (for instance - CHCS requires a telnet connection);
  - limit access to specific applications (users should not use the MTF as an alternative Internet service provider unless specifically authorized);
  - configuration options that will require or avoid a dial-back modem capability (require when fixed user, decline when mobile user identified);
  - other configuration options as appropriate.
- operational alternatives for RADIUS, i.e.:
  - fully distributed and autonomous - each server is administered by the MTF providing the service;
  - distributed and cooperating - each server administered by the MTF with alternative default servers mirroring subscriber profiles and services;
  - centralized - single or selected servers administered by a central authority with input from sites served;
  - remote operations;
  - other alternatives as appropriate.
- installation and operation:
  - demonstrate how to initiate, configure (set/restore user options) and operate;
  - discuss ease of installation, operation and configuration;
  - discuss feasibility of remote operations and demonstrate if appropriate;
  - how to use and maintain audit logs to include exception processing of logged entries;
  - assessment of requirements for user configuration initialization and maintenance.

**Deliverables to the sites:**

- a set of recommended operational procedures

- a demonstration of capabilities given alternative configurations, both dial in user configuration and server operations configurations
- a training presentation that guides the demonstration to include - objective, demonstration, findings, recommendations for major areas, e.g., operations, user configuration, RAS configuration, installation and maintenance.

TABLE OF CONTENTS

***I. Introduction*** ..... 61

    Background ..... 61

    Purpose ..... 61

    Report Organization ..... 62

    Intended Audience ..... 62

***II. Information Security Evaluation (ISE) Process*** ..... 63

    Participants and Roles ..... 63

    ISE Process Overview ..... 63

    ISE Investigation at a Medical Treatment Facility ..... 64

***III. Observations and Recommendations*** ..... 66

    Organizational Climate ..... 67

    Security of Patient Information ..... 70

    Security Policy and Procedure ..... 74

    Staffing Support Impact on Security Policy and Procedures ..... 77

    External Access to MTF Systems and Applications ..... 80

    Systems Administration ..... 83

        Systems Administration - Configuration ..... 83

        Systems Administration - System Services ..... 85

        Systems Administration - Network Operation and Services ..... 86

        Systems Administration - Passwords and User Accounts ..... 87

    Training ..... 90

    Disaster Recovery and System Backups ..... 92

    Physical Security ..... 94

## **I. Introduction**

### **BACKGROUND**

The United States Congress, the Secretary of the Army, and the Chief Information Officer of the U.S. Army Medical Command recognize the current vulnerability of medical information systems to attacks on the integrity and confidentiality of healthcare information. To address these issues, Congress recommended a program that develops and demonstrates securing of healthcare information systems.

Healthcare Information Systems are required to create, store, access, and exchange sensitive but unclassified information as part of their normal regimen. The challenge is to handle the information in such a way as to protect the privacy, confidentiality, and integrity of the data while still providing efficient and effective access to authorized users when and where needed. To meet this challenge and integrate the policies, procedures, methods, and technologies into existing military or healthcare information systems requires the following:

- An understanding of the present state of the information security within the healthcare community;
- An analysis and documentation of functional requirements to provide requisite security while minimizing impact on required operational effectiveness; and
- A demonstration in the healthcare domain by installation and operation of a prototype to evaluate the effectiveness and operational impact of proposed security improvements.

The purpose of the Defense Healthcare Information Assurance Program (DHIAP) is to develop and field prototype systems that provide reliable access to healthcare information while protecting that information from unauthorized access or alteration. The initial step in accomplishing that purpose involves evaluation of existing medical information systems to determine vulnerabilities in information assurance capabilities and to make recommendations for operational procedures and policies to address those vulnerabilities.

This report provides the results from the evaluation and assessment phase of the program, in which selected medical information systems were evaluated to determine vulnerabilities in existing information security capabilities.

### **PURPOSE**

The purpose of the Defense Healthcare Information Assurance Program (DHIAP) Composite Evaluation Report is to provide the results from the Information Security Evaluation (ISE) effort of Phase I of this program. This effort builds the roadmap for follow on work in DHIAP and identifies information assurance areas that will benefit from command attention. It lays out the observations of vulnerabilities and risks as well as recommendations from the DHIAP team to address the observations. It identifies areas that should be addressed at the Medical Treatment Facility (MTF) level and areas that lie within the responsibilities of

organizations with system wide authority. Some of the vulnerabilities identified will be resolved through the continuing efforts in subsequent phases of DHIAP.

## **REPORT ORGANIZATION**

During the period January 1999 through June 1999, the Defense Healthcare Information Assurance Program (DHIAP) team conducted Information Security Evaluations at designated government sites. This report presents the process used to evaluate the sites and observations with associated recommendations derived from the evaluations.

It is necessary to detail the process used to conduct the evaluations in order to validate the findings and recommendations. This process is outlined in Section II below and detailed in Appendix A. Appendix A also includes a survey adaptable as a checklist for all MTFs to determine whether or not they may be vulnerable to some of the same areas of concern noted by the DHIAP team in the evaluation of the information security systems discussed in this report. Appendix B identifies and lists the credentials of the evaluation team members, both organizational and individual. Reference documents used to increase the DHIAP team's understanding of the existing and planned operations, policies and procedures are listed in Appendix C, and Appendix D is a listing of acronyms and abbreviations found in this report.

Results from these Information Security Evaluations were provided to the individual sites in the form of site-specific observations and recommendations as part of an evaluation exit briefing. As explained to the sites, the observations and recommendations point to general areas and specific issues that the DHIAP team noted during the course of the evaluation. Exceptions to the negative comments were found but the problems noted were sufficiently pervasive or significant as to warrant mention.

Section 0 contains observations and recommendations related to findings that the DHIAP team felt deserved more command attention than could be provided by the MTF. The observations and recommendations are generic enough as to apply to other MTF. In many cases these risks and vulnerabilities required more than the ability or the authority of the individual MTF to address and resolve since the issues identified deal with potential system-wide impact on information security.

## **INTENDED AUDIENCE**

This report is intended to serve as a report of risks and vulnerabilities found and recommendations for mitigating those findings. It became evident in the development of the report that there exist multiple audiences for the information contained herein. The observations and recommendations apply not only to the facilities evaluated but could affect the daily operations of any MTF. Other sites may be interested in this report as a resource for identifying and addressing immediate operational problems or concerns that may exist within their own systems. Additionally, the sites evaluated made it clear during the presentation of findings all problems were not in the scope of their authority or ability to address. Thus, this report addresses an additional audience - those entities that have larger, regional or command authority and responsibilities. It is the DHIAP team's hope that the observations and recommendations provide sufficient clarity to support command attention required to resolve the issues identified.

## II. Information Security Evaluation (ISE) Process

This section provides a synopsis of the Information Security Evaluation process as it was adapted and applied to the MTF participating in the DHIAP.

### PARTICIPANTS AND ROLES

The DHIAP ISEs were conducted under the auspices of the Telemedicine and Advanced Technology Research Center (TATRC) of the Medical Research and Materiel Command (MRMC). Members of the DHIAP team of information protection, security, and healthcare experts included:

- **ATI** (Advanced Technology Institute): Information Protection Solutions group
- **LMES** (Lockheed Martin Energy Systems): Data Systems Research Division
- **SEI** (Software Engineering Institute): CERT Coordination Center
- **HOST** (Healthcare Open Systems & Trials) consortium
- **ADL** (Arthur D. Little, Inc.): ISE Team coordinator
- **Government representatives** from TATRC/MRMC

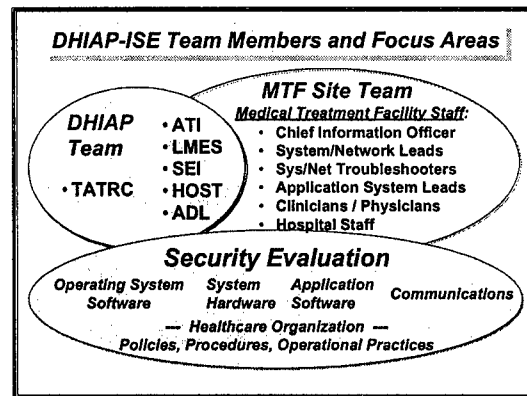


FIGURE 1 - DHIAP-ISE TEAM MEMBERS AND FOCUS AREAS

In addition, each Medical Treatment Facility (MTF) included in an ISE contributed the time of its Information Management staff, healthcare administrators, and clinicians. **Figure 1** above illustrate the organizations represented on the DHIAP team, the types of team members contributed by each MTF involved in an ISE, and the major subject areas addressed in the ISE process.

### ISE PROCESS OVERVIEW

The overall process planned for the DHIAP Team was to investigate security vulnerabilities at a representative set of military Medical Treatment Facilities (MTF), as shown in **Figure 2**. After TATRC identified two MTFs for evaluation in Phase I of the DHIAP, the team worked with

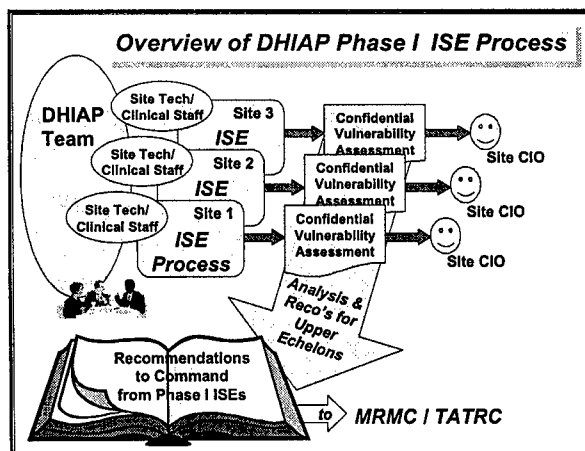


Figure 2 – DHIAP ISE Process



designated staff of each MTF being investigated to perform the sites' ISEs. Each ISE investigation concluded with several forms of feedback to the site, as follows. A Site Vulnerability Assessment briefing outlined the team's observations and recommendations of instances where site information was found vulnerable to exposure. This briefing was confidential to the MTF site and was provided to MTF leadership, the Chief Information Officer (CIO), and selected staff of the Information Management group. Supporting details and recommendations for specific technical issues were provided to the MTF staff during the course of the evaluation. Subsequent to the briefing, a report providing technical details specific to the system and network administrators was provided to the CIO.

Following completion of the scheduled Phase I ISEs, the DHIAP team clustered the observations from each site in various ways to identify information threats and vulnerabilities common to all sites. The result of that effort is this report of observations and associated recommendations outlining the major vulnerabilities encountered and the DHIAP team's recommendations for actions to address the vulnerabilities.

**ISE INVESTIGATION AT A MEDICAL TREATMENT FACILITY**

ISE activity at an MTF site began with site nomination and selection. TATRC nominated a number of representative sites, explained the incentive for the nominated sites to participate, and requested initial site information to screen the sites down to a representative sample. The request for information took the form of a Preliminary Survey requesting basic information about the nominated sites' staff, installed systems, existing policy, current training, and current practices. Based on survey responses, TATRC, with the DHIAP team, selected two MTFs to be the sites initially evaluated in the ISE<sup>1</sup>. At each facility, the ISE team followed the process and general timeline that is shown in **Figure 3** and described in detail in Appendix A to this report.

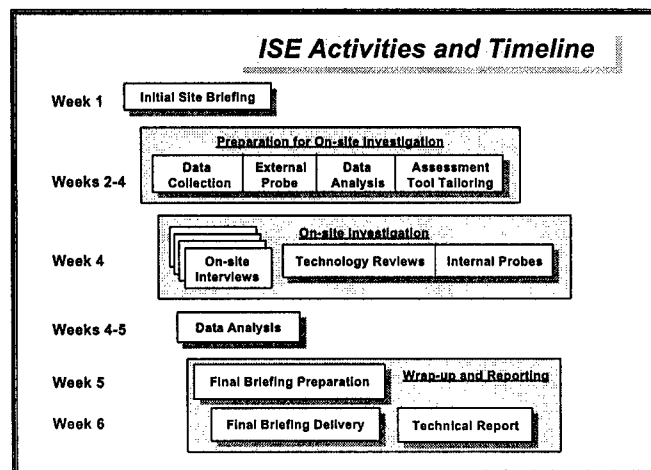


Figure 3 - Timeline and Activities of ISE

<sup>1</sup> Note: two ISEs were planned at one of the sites, making a total of three ISEs, but the third ISE was deemed unnecessary.

The DHIAP Team concluded the evaluation activities by analyzing the observations and recommendations developed during all of the ISEs and developing Phase I summary materials and Phase II plans. This Composite ISE Report documents the Phase I summary of the types of vulnerabilities currently evident in the military MTFs and DHIAP recommendations for MRMC/Upper Echelon actions.

### **III. Observations and Recommendations**

The observations and recommendations that follow are derived from the DHIAP team's site evaluation. These results have been previously provided to the evaluated MTF in the form of a formal presentation followed with specific technical information detailing particular system configuration issues found along with recommended mediation.

This report contains no site-specific information and should not be construed as a report on or about specific sites. Rather it is based on the assumption that for the types of sites evaluated the vulnerabilities encountered will be generally applicable. Likewise, the recommendations are not just applicable to single sites but rather address areas of concern at the organization and system levels.

The format used in the report is organized to provide the reader with context and focus within a significant area. There are twelve categories that organize the observations and the associated recommendations. The coverage for each category begins with a paragraph description/definition providing context for the remarks that follow. A management objective is associated with each category. This management objective should be interpreted as a standard to strive for in the area.

The observations are narrative descriptions of the potentially risky conditions, practices, and/or procedures that the team observed during the course of the evaluation. While in most cases, exceptions to the observations can be cited, the problems identified were sufficiently pervasive as to merit attention.

Observation specific recommendations for each category are directed toward an appropriate focus of responsibility and authority. The recommendations are tied to the context of the associated observation. In some cases a recommendation is applicable to more than one observation area because of the high interdependence of the systems examined and the overlapping nature of mediation actions. In those cases recommendations may be somewhat redundant in order that each observation-recommendation set can stand alone as an action area.

**ORGANIZATIONAL CLIMATE**

We define organizational climate as the attitude that permeates an organization regarding a particular matter of command and organizational interest. It is the ability of the organization to understand and interpret the intent of a policy because the guidance is ingrained throughout the organizational practices. The DHIAP team based their observations in this area on interviews, structured and one-on-one, with the staff from all areas of the MTF.

**MANAGEMENT OBJECTIVE:**

**Information Assurance policies and procedures are understood and endorsed throughout the organization. Members of the organization understand and support the policies and procedures well enough that they have no doubt how to react in situations not specifically covered by the existing guidance.**

***OBSERVATIONS:***

The DHIAP Team observed a consistently strong organizational ethos concerned with the security of sensitive healthcare information. However, the DHIAP team also observed a sense of frustration with the implementation of guidance that would support that concern. The DHIAP team concluded that information security was accorded low priority based on the lack of clarity in information security guidance, the perception that emphasis on information security was often more form than content, and observations of apparent variations in application of security policies. This perceived lack of commitment to information security was manifested by the frustration the staff felt in trying to enforce policy that was largely unwritten and therefore situation dependent. One member of the DHIAP team observed that knowledge of security policy was being transferred as part of oral tradition.

The fact that the standards are unclear and unmeasured seemed to be the results of two attitudes prevailing within the sites' hierarchy: first, responsibility for implementing security in mandated systems belongs solely to the owners of the mandate and, second, that implementing sound security practices would conflict with "getting the job done." The first belief results in widespread reluctance to deal with the problems within the compass of their local authority, knowledge, skills and ability. It is not a shirking of responsibility so much as a ready acceptance of deferral of responsibility to higher echelons (USAMISSA, TIMPO, MEDCOM, etc.). The second attitude mentioned above results in any conflict between mission and security resolving in favor of "the real job." The perception is that MTF leadership believes security to be too costly or burdensome compared to gains from enforcing it. This leads to exceptions becoming the norm. These two attitudes appeared to be used to justify shortcuts in lieu of addressing the issues where security is either impacted or perceived as a burden to operations.

Where individuals are aware of a security policy, there was a perception expressed that it is applied unequally (e.g., an observation that Physicians have special status, are given special considerations for adherence to documented policies or mandated systems, and are not subject to the same security guidance). Staff frustration was fueled by observing that systems provided by outside organizations varied significantly in their ability to consistently support the desired level of protection for sensitive information. It was also frustrating for support

staff to deal with their perception that privileges and prerogatives associated with medical and military rank supplanted individual responsibility for security and a tolerance for the shortcut solution.

***RECOMMENDATIONS:******Higher Echelons – Support for Security Policy and Procedures:***

1. Establish information security as a Medical Command priority.
2. Institute a Command-wide information security education/awareness program to increase staff understanding of risks.
3. Establish command wide security requirements for user access, user identification and password, auditing, information security, remote administration, and secure use of the network-enabled tools such as e-mail and Internet.
4. Provide defined policy for information security and related issues for Command and MTF activities.
5. Assure that all levels plan to employ security practices appropriate to the risk.
6. Implement procedure to assist the MTF management, healthcare, and IT Group efforts to define more detailed policies and procedures for enforcing and monitoring compliance with security practices. Review policies and procedures developed to assure they fully support the Command's security initiative.

***Higher Echelons – Support for Computer Systems:***

1. When selecting information systems provided by outside organizations, assure (via contract) that:
  - The delivered system will meet established security requirements (see recommendation 3 above) for user access, user identification and password, auditing, information security, etc.
  - Implementation services will include adequate training and documentation for both user and systems support.
  - Ongoing system support/maintenance provided by the outside organization will comply with established requirements for using secure communication methods and maintaining confidentiality of patient information.
2. Develop standards to be followed by organizations outside the MTF (e.g., MEDCOM, TIMPO, USAMISSA, Tri-Care contractors, and third-party vendors). The standards should address the level and types of required system implementation support they are to provide to the MTF (e.g., resource planning for implementation and ongoing use of the system; analysis of operational impact of the system and the need for changing MTF security and operating procedures; resource planning for installation, use, and maintenance of hardware/software delivered with the system; etc.).
3. Provide resources necessary to support the implementation and ongoing use/support of the system at MTF.

**MTF Management:**

1. Define operational standards with which new and existing systems must comply. These standards should be based on higher echelon guidance modified as required to incorporate local requirements.
2. Isolate those systems that do not comply with established standards from the other systems within the network in order to maintain system-wide standards.
3. Conduct internal campaigns to keep MTF staff and employees aware of the MTF Command's commitment to information security.
4. Assure that security procedures are equally applied to all levels and all types of MTF personnel and that exceptions are requested and handled in an official forum that leads to formally documenting resolution of the requests.

**SECURITY OF PATIENT INFORMATION**

This section collects information based on the team's formal and informal interviews with MTF staff about the organization's ability to secure sensitive patient information. The challenge in the MTF environment is to make the right data available at the right place and time to support the caregiver's information needs while protecting the patient's right to privacy and confidentiality.

**MANAGEMENT OBJECTIVE:**

**Patient information is available only to authorized personnel at the time and place needed. Authorized access is based on user's identity, authorization, and need with regard to work to be performed at that time and at that location. Unauthorized access is precluded.**

**OBSERVATIONS:**

MTF staff expressed concern about the lack of a comprehensive policy on patient privacy and confidentiality of patient information. They pointed out that patient information may be exposed in many ways including: providing patient information telephonically to outsiders with minimal verification of the identity of the receiver/requestor; using non-secure e-mails to transmit patient information; accessing patient records from remote locations via public Internet; and leaving patient sign-in sheets in view of waiting patients and other visitors. It was pointed out in the interview process that there has been an increase in demand for access to patient information by non-MTF sources, and it was felt that responding to these requests for access increased the risk of unauthorized exposure of that information. Examples of external access to patient information include transferring patient information to managed care contractors and satisfying the increased requests for production of "ad hoc" reports.

The staff's concerns apparently stemmed from the mismatch between their understanding of how patient records should be protected and their impressions on how the records were actually handled. There appeared to be three main areas of concern: 1) access by external, and therefore suspect, agents; 2) impact of technology on tracking and controlling access to sensitive information; and 3) the issues of patient permissions.

At the MTF, sensitive patient-identifiable information in electronic format was identified as at risk for exposure in a number of ways. Internal to the MTF, the Medical Staff members maintain "convenience" files of patient information on their own or their departments' computers. These unofficial personal databases are not subject to the IT Group's official policies for protection, purging, and quality checking. Also, in normal day-to-day use of applications such as CHCS, the personal computers used as terminals hold patient information in cache memory as a normal byproduct of their use for system access. External providers, the TriCare contractors and third party vendors who provide technical support for MTF systems/applications also have access to MTF patient data. This generated questions of controls and tracking applied to outside agents to prevent unauthorized release of sensitive information. It became clear that the level of trust inherited by members of the MTF staff was not necessarily extended to those outside the MTF whose duties granted them extraordinary access to sensitive information.

The concern expressed by the staff illustrates a unique attribute of military medicine that needs to be considered; military staff invest a significant amount of trust in the systems that support them. Military members and dependents, even though surrendering some personal prerogatives when they join the military, absorb the culture of trusting the military to protect the letter and the spirit of their implicit agreements. If that faith should be broken by such incidents as third party contractors marketing information on military members to outside agents, then a special trust will have been violated. Although not articulated, it appeared that MTF staff wholeheartedly accepted the responsibility of honoring the trust their clients vested in them and worried about fulfilling the obligations of that trust.

Patient information recorded on paper is also exposed to risk. Clear management of disposition of printed patient information is weak, whether printed in authorized mode from the MTF patient care computer systems or printed from the Medical Staff's unofficial computer databases and systems. Other types of paper records, such as ADS "Bubble Sheets," are not covered well by management/disposition policies.

Apparently one of the reasons for the staff's discomfort is a lack of appreciation for the limitations and capabilities of the technology. It became clear that the pace of technology changes had outstripped policy guidance and the staff's ability to assess the impact of change on their operations. The challenge with paper records had been to track them, provide physical security, and manage the flow of documents from record repository to care giver and back to the repository; the rules were clear and relatively easily understood. With the advent of the hybrid record, some paper and some electronic, the rules have changed, and the capability to understand and control proliferation of sensitive material is not as clear. As change is introduced it becomes clear that not only must security of patient information be considered but also staff comfort level with that security must be addressed.

One other subject expressed as a concern in this area was confusion about the proper handling of patient's permissions. There was concern that patients understood neither the permission documents they were asked to sign nor what they were allowing to occur when granting blanket permissions. There was also concern expressed about the coverage of those permissions, e.g., are third party vendors covered by the same set of permissions and related restrictions as the MTF? The staff felt they have an obligation to the patient to ensure that the patients understand the meaning and ramifications of the permissions they are asked to grant. The DHIAP team was left with the impression that one of the reasons the staff expressed the concern was that the rights accorded to the military member who agreed to permission statements was unclear.

***RECOMMENDATIONS:******Higher Echelons – Support for Security Policy and Procedures:***

1. Clarify rights accorded to military members regarding permission statements particularly in respect to pending legislative mandates, e.g. HIPAA.
2. Provide guidance and appropriate workstation software to sanitize cache memory after sensitive information downloads.



**MTF Management:**

1. Define a comprehensive MTF policy for protecting patient privacy and the confidentiality of patient information to include requirements for patient permissions.

**IT Group Management:**

1. Develop a vulnerability profile outlining MTF-approved and unapproved methods by which patient information is shared with outsiders (e.g., telephone, fax) or might be exposed to outsiders/unauthorized MTF staff (e.g., open display of clinic patient sign-in sheets, unattended terminals involved in active sessions, etc.).
2. Define detailed policies and procedures to specifically address all situations noted in the vulnerability profile. Some known subjects to be covered by detailed procedure include the following.
  - Verifying the identity and security profiles of individuals who request new/modified access to systems and who request ad-hoc reports that include patient-identifiable information (including individuals who represent the external providers/maintainers of MTF systems, e.g., staff of MEDCOM-TIMPO-USAMISSA, Tri-Care contractors, and third-party vendors)
  - Assuring that third party payers are given only the information they are authorized to receive based on their contracts with the patient and the MTF
  - Verifying the identity of outsiders who request and/or are given patient information via telephone
  - Tracking receipt and disposition of information faxed and/or mailed to outsiders to assure proper procedure is followed
  - Securing e-mail transmission of patient information outside the Command
  - Including in the facility's portfolio of supported systems those MTF staff "convenience files" that are deemed necessary to providing quality care and make them subject to the same access and information protection procedures (e.g., audit compliance, backup/recovery, purging, etc.) as the "official" MTF systems.
  - Assuring that personal computers allowed to access patient information (e.g., CHCS terminals) do not retain the patient information in their cache memory when the session has ended
  - Tracking use and disposition of paper copies of sensitive patient information (e.g., system-generated reports, forms completed by/for the patients, ADS bubble sheets, patient sign-in sheets)
  - Tracking existence of non-standard software installed on MTF systems, determining whether they should be allowed, and assuring they do not have an adverse impact on overall processing of MTF systems
3. Review and reinforce procedure and practice for obtaining, retaining, and using patients' permission/authorization for release of information from their files.
4. Publish the new policy and procedures for assuring physical security of the MTF patient information and train staff in its use. To reduce the perception that rules are administered

*DHIAP PHASE I COMPOSITE EVALUATION REPORT- WORKING DRAFT*

differently depending on staff role or other differentiator, assure that enforcement of the new procedures is evident to all staff members.

5. Provide training and familiarization on new technology in the form of fact sheets for staff.

**SECURITY POLICY AND PROCEDURE**

Security policy and procedures are the tools an organization uses to implement information security practices. The policies provide the operational guidance for protecting sensitive information and form the basis for commonly accepted practice within an organization. The procedures address particular actions required and must be adapted to the operational needs and realities of the target organization. The DHIAP team reached the following conclusions after examining published documentation that defines acceptable practices at the site and interviewing members of the staff and users about their understanding and implementation of practices.

**MANAGEMENT OBJECTIVE:**

**Policies and procedures dealing with information assurance are sufficiently comprehensive that necessary exceptions are minimal. Personnel impacted by the policy are familiar with and follow its guidance. Procedures are applicable to the systems and operations addressed and are updated periodically to conform to changes in the environment.**

**OBSERVATIONS:**

In general, the DHIAP team observed a disconnect between the policy and its implementation and varying degrees of frustration with policy implementation and enforcement. MTF policies often rely on individual interpretation and real-time, verbal guidance. This appeared to be the result of fragmented, incompletely documented, and inconsistently administered information security policy.

The technology implemented in the MTF IT environment is changing so rapidly that policy and user training are not keeping pace. Also, the degree of variance in the mandated systems' approaches to security affects the ability to create universally applicable policy guidance.

Operational necessities were often used as a rationale to bend security policy. Because operational considerations are used as justification for bending policy, exceptions to policy enforcement make the policy itself appear inconsistent. It appeared that the policies were being redefined based on situational conditions and there was frustration over defining acceptable and unacceptable behavior.

There appear to be many causes for the observed incongruous state of policy and procedures including: dependence on multiple contractors and subcontractors; variable, system dependent training in security practices; delegation of responsibility for enforcement to the lowest possible level; and perception of a conflict between operational needs and sound security. The missing element appears to be an institutionalized process regarding information protection that consists of uniform security policies, procedures, and practices.

Policies for the following areas are in need of clear definition and implementation as operational procedures:

- **Systems**: Users and system administrators must often adjust MTF operations to fit with the characteristics of a particular system and/or develop unique approaches to security as a result of situations unique to the various installed systems.
- **User Environment**: Users who are unaware of the impact of security policies on operations increase the risks associated with sensitive information. As they retrieve information to their local system for operational convenience or fail to log off workstations, they compromise system/network access controls. Instances of unattended "active" terminals, use of access "work-arounds," and use of broad, role-based access authority all contribute to allowing the user community inappropriate access to patient information.
- **User Convenience Practices**: "Convenience" practices of some system users (e.g., clinical staff maintenance of unofficial hardcopy and electronic patient data in files that are outside of system control) jeopardize information security. It is common for some individuals to download patient information to local storage on unsecured systems, leading to risks of unauthorized access and use of inaccurate or out-of-date information. Also, some users intentionally work around planned controls when using the authorized systems; for example, the practice of sharing CHCS sessions.
- **Internet Access**: Many MTF staff members do not understand the security risks associated with downloading information from the Internet and do not appreciate the impact of such activity on bandwidth available to the facility. MTF policy needs to be reviewed to ensure that Internet usage is sufficiently addressed. In addition, MTF staff members should receive regular training on the use of the Internet.

At the system level, the organization's incident reporting procedure varies by system and organizational level and is not well understood. There is no facility-wide procedure for the tracking and follow-up of reported violations and little systematic monitoring to detect unauthorized hardware and software.

***RECOMMENDATIONS:******Higher Echelons – Support for Security Policy and Procedures:***

1. Provide templates as examples of security policies that multiple MTF can adapt for their use. These documents should accomplish two tasks: address information security at the operational level, and illuminate the variety of approaches to security that operational components must presently deal with.
2. Mandate standardized approaches to security for the functional systems in operation at the MTF in order to provide an expected mode of operation for all users and administrators.

***MTF Management, with guidance from MTF IT Group Management:***

1. Define and approve MTF policies and procedures for information security that comply with the policies and priorities set by higher authority. Assure that policies are sufficiently clear to support proper definition and consistent application of procedure.
2. For those areas where the practices are ambiguous or contradictory, identify and work with higher authority to clarify and standardize.

3. Assure that procedures identify responsibility and that the responsible position carries appropriate authority.
4. Define and implement formal procedure for assuring policy compliance. Include instructions for reporting and processing security violations, applying appropriate action, and tracking/following up on reported violations.
5. Define and implement procedures for requesting exceptions to approved policy and procedure. Include instructions for filing the request, for documenting reasons and terms related to any permission given, and for performing follow-up checks to assure that the permitted practice does not cause exposure of sensitive information. Include in the review process for exceptions the examination of the reason for the exception. Exceptions may indicate that some systems are operating out of the set and agreed bounds.
6. Establish "sunset" provisions for each exception granted including the duration of the exception and the conditions that cause revocation of the exception granted. The end goal is to understand the rationale for exceptions and, if necessary, grant temporary exceptions until root causes are addressed.
7. Establish procedure to periodically review the effectiveness of existing policies and procedures. The intent of the periodic review should be to identify and address systemic problems. Include in this a review of risks introduced since the last review (e.g., changes to departments'/staff members' responsibilities, physical changes to the facilities, evolutionary changes to capabilities of internal/external hardware and software, etc.).

**STAFFING SUPPORT IMPACT ON SECURITY POLICY AND PROCEDURES**

Staff resources dedicated to formulating, implementing and monitoring security policy and practices need to be adequate and they need to provide defined guidelines of responsibility and authority. They should receive sufficient technical and general training to competently carry out their responsibilities. Staff resources with operational responsibility impact on the organization's ability to follow stated security policy. If the staff is not aware of appropriate information security procedures, or if staff is under-resourced and over-tasked, then the priority for protecting sensitive information will slip. The DHIAP team based their observations on observations made while on site and on interviews with MTF staff.

**MANAGEMENT OBJECTIVE:**

**Staff resources are assigned responsibility for information security and given authority to implement security policy and procedures. The actions of operational staff users are in compliance with stated information security policy and procedures.**

***OBSERVATIONS:***

Staffing support affects two areas: operational support to the functional elements, and security staff support to the entire organization.

***Operational Support Functions:***

The application systems that support the MTF primary functional requirements are often mandated by organizations outside of the MTF, such as MEDCOM, TIMPO, and USAMISSA. Department Units within the MTF often inherit the operations and maintenance of mandated systems supporting their departments. The responsibility for information security is usually assumed along with the operational responsibility.

The DHIAP team found that the staff members responsible for operating functional systems were not well-grounded in accepted information security practices. The strategy observed was assignment of experienced functional users to manage these mandated systems with a reliance on centralized remote administration augmented with books of detailed routine instructions for local operations. The weakness with the implementation of this strategy is that system managers, although experienced in the functional area, have limited systems administration background and therefore are not well equipped to determine policy or set procedures. This is compounded by the lack of standardized policy guidance and the limited resources directed toward information security.

The myriad of systems also impacts the IT resources with unique, changing, or increased demands on staff resources. For example, technical system administrators have to adapt to manage a variety of system configurations; application and technical troubleshooters are required to respond to multiple systems; and application users must respond to a number of differing system operations policies. Limited training is provided to enable the various MTF staff to adequately meet these responsibilities, and little or no consideration is given the MTF for handling the extra costs (user and technical staff resources, implementation process, training, materials) associated with implementing the systems.

**Security Staff Functions:**

The DHIAP team viewed the security staff as consisting of those assigned primary staff responsibility for security and the staff members augmenting that area. Technical assistance support staff included security in their oversight and assistance duties. Functional staff members were assigned as additional duties the task of liaison with the IT staff in matters regarding system operations and security.

The DHIAP team observed confusion about the roles, work responsibilities, reporting responsibilities, and authority of MTF departmental staff who are assigned to support the security function. Where the function of Security Manager has been established, the role has been given responsibility with limited authority and control, making it difficult or impossible for security staff to meet the security requirements. The security manager has limited training and experience in security practices and technology. Staff members augmenting the security department were found to be inexperienced in the information security area and have only limited training. Generally, training available is the same as given to users and training in technology-specific areas (e.g., "Introduction to NT") is limited.

Security staff is often assigned multiple duties and responsibilities, stretching resources and creating priority conflicts. Available staff time is not sufficient to competently perform the work (e.g., password management) that assures compliance with security policy.

In general, MTF lack sufficient dedicated resources to implement stated security policies and to effectively monitor compliance. The dedicated resources need to be augmented by knowledgeable and motivated staff.

**RECOMMENDATIONS:****MTF Management:**

1. Evaluate staff responsibilities for potential realignment. System managers should be responsible for meeting mission requirements of the systems they manage. They should have ready access to guidance on matters dealing with sound security practices from the IT staff experts. The operation of the systems, while under direct control of the functional organizations, should receive close supervision and monitoring from the IT staff.
2. Define the department structure, job responsibilities, staffing, and staff credentials/experience necessary to carry out the MTF security responsibilities<sup>2</sup> as defined in MTF security policy/procedure and the accreditation package. Document plans for use of staff from other departments as appropriate. Where the defined organization structure is considered inadequate to carry out all responsibilities, negotiate with Command, MTF and departmental leadership to assure adequate coverage of subjects suspected to represent the highest risk to the MTF.
3. Assure that early planning for new systems to be implemented at the MTF includes a review of the staff and skills required for supporting and using the systems. Identify how the MTF will meet all skill/staff requirements, and assure formal arrangements are made

---

<sup>2</sup> There should be at least one individual assigned with the responsibility for system security. That individual should have sufficient expertise to advise the commander on matters that will adversely impact the MTF security. Along with the responsibility for system security, the responsible individual should have authority to develop and mandate necessary policy to address the significant areas of risk facing the MTF.

to provide staff to: install/test the system and train users, provide ongoing technical system support, provide ongoing user assistance and troubleshooting, perform timely password maintenance, etc.

4. Make the secure operation of the various systems a matter of command interest as a failure in connected systems may impact the entire system.

**MTF Security Department Management:**

1. Develop and enforce standard policy dealing with the details of operating interdependent systems in a secure manner.
2. Develop and deliver training for departmental security staff on MTF security policies and procedures. Provide extensive orientation on the MTF facility and operational policies and procedures and on information security shortcomings and problems experienced in the past, and provide full information about regulations and outside authorities (e.g., accreditation package) to which the MTF is responsible.
3. Based on results of a skill assessment, develop the expertise of the dedicated security staff as needed in areas integral to their job responsibilities (technical security of systems, development of security policy and practices, MTF departmental processing, technical subjects such as networked communications, etc.).
4. Negotiate with departments whose staff performs security-related responsibilities (e.g., to serve as Terminal Area Security Officers) to: agree on the work to be done, allocate adequate staff time for the work, and define the reporting responsibilities to the home department vs. the IT Group.
5. Periodically review the security organization's structure and responsibilities in relation to changes in the MTF organization. As appropriate, work with MTF management to alter security policy and/or security staff responsibilities and techniques to correspond more closely with the priorities and flow of work of the MTF.
6. Provide initial and refresher training to MTF staff on the facility's security policy and procedures. Training should be refreshed when the procedures change and whenever personnel are assigned new duties. Incorporate security training into the MTF annual training program.



**EXTERNAL ACCESS TO MTF SYSTEMS AND APPLICATIONS**

Access to the MTF systems and applications should be readily available to support operational requirements. It should also be accomplished in such a manner that sensitive information such as patient data is not exposed during transit or at the remote location. System integrity, i.e., the ability to control access to the internal system and to monitor user actions, should not be compromised by external access. The DHIAP team based their observations on an examination of three primary objectives of remote access: access to patient information; access to electronic mail and other office automation type support functions; and administration and maintenance of systems and applications from centralized locations.

**MANAGEMENT OBJECTIVE:**

**Remote access to the internal systems will not compromise the integrity, security, or availability of healthcare information, the systems, or the network.**

***OBSERVATIONS:***

The DHIAP team observed that medical information systems at the MTF have evolved into an interdependent system of standalone systems. Systems with varying degrees of certification (DOD Standard 5200.28) interconnect with each other, with other DOD and MEDCOM elements through the DISA networks, and to the rest of the world via the Internet. This results in a powerful capability that carries with it some significant risks: a physician can connect to the Internet via the local commercial Internet provider, telnet to a CHCS system, and review patient data at home. However, passing sensitive but unclassified data across commercial circuits with no security violates both Army security guidance and the Privacy Act.

The paths provided for the doctor's use in the above example also provide a path for potential compromise of security or integrity. Information passed over the interconnected systems, and therefore at risk, includes user ids and the associated passwords. A determined intruder could pose as an authorized user and exploit a captured user id and password to access patient medical records, provider data, and entire medical databases. Further, once the system has been penetrated, an accomplished hacker could use the compromised system as a pathway to other military medical systems both those located within the MTF and those connected to the MTF via the trusted medical network. At the time of the DHIAP visit, no measures for securing the Internet traffic or the patient traffic were in effect.

It should be noted that the MTF examined are no better or worse than many other commercial and government organizations. The growth of capabilities supported by emerging technology has outstripped the maturation of high level guidance and direction on implementing secure Internet and networked technology. While technology exists to provide security for sensitive information while in transit, implementation would require changes to user and system interfaces. Those changes have been deferred pending revision of the primary military healthcare systems.

A separate issue from using unsecured communication for operational support is the issue of remote access for administration and maintenance. In several cases, System and Network

Administrators who have privileged access are outside MTF Command authority, with responsibility for systems' operations broadly distributed across the MEDCOM. A sound economic rationale is that it is easier and more economical to train a small cadre of technical experts at a central location than it is to train administrators at every system site; the issue here is one of safe practices. To gain access to the systems being maintained requires passing root or super user identification and passwords across the connecting network. A determined intruder could capture those user ids and associated passwords using them to compromise the entire interconnected system. Using the public network with security control limited to that provided by the MedNet frame relay could expose the proverbial keys to the castle.

Remote administration also introduces the questions of responsibility and authority for ensuring secure operations of the mandated systems, and of the controls that should be applied for those systems to connect to a trusted network. The MTF will be held responsible for the safe operation of the network, the systems attached to that network, and the sensitive information accessible on that network although they have little or no control over remotely located unknown agents. Where a third party performs software installation, there is no standard procedure for giving and removing access to the installer or for ensuring compliance with MTF policies and procedures. Since the externally administered systems are treated, in most instances, with the same trust as others on the network, i.e., not isolated from the "trusted" systems, there is some concern that outside administrators could gain access to trusted systems. It was reported that locally introduced changes to increase security were undone by the remote agent. There is also some concern that outside administrators could gain access to information beyond the boundaries of the maintained systems.

The remote system administrators perform some work in a manner that is unsafe. Insecure methods in use for remote system administration include shared passwords and absence of techniques for encrypted authentication and verification. In a number of cases, MTF personnel have only limited knowledge of some of the systems they support. They lack the training and skills necessary to understand, monitor, and audit activity on such systems, and do not always have the time to carry out their responsibilities.

It appears to be common knowledge at the MTF that allowances are made to relax security in order to promote operational efficiency and effectiveness. While the operational need makes sense, little work has been done on exploring alternative approaches that would provide the required operational capability without endangering the system and information security.

***RECOMMENDATIONS:******Higher Echelons – Support for Security Policy and Procedures:***

1. Establish command guidance for providing and managing remote access. That guidance should include programmatic guidance directed at ensuring strong identification and authentication of remote users and protection of sensitive communication from interception.

***MTF Management:***

1. Establish local policy and procedures for Internet access via MTF system resources.
2. Establish local policy and procedures for remote access via Internet or dial-in to MTF systems.

***IT Group Management:***

1. Secure critical network resources (e.g., DNS, routers, and bridges) from external access.
2. Isolate remotely administered systems from each other and from the MTF network. Ensure that existing trust relations<sup>3</sup> with remotely administered systems are well understood and approved.
3. Implement use of strong identification and authentication techniques for remote access to all systems.
4. Implement a procedure for working with external individuals who must remotely administer MTF systems. Include requirements to: acquire certification of "trusted status" (need to know) for each request for access to the system; assure outsiders are aware of and comply with MTF policies and procedures; and audit remote access transactions for compliance with MTF procedures.

---

<sup>3</sup> A trust relation is a willful granting of trust from one party to another. In this case the trust relationship deals with the question of how much the MTF, who is entrusted with the security of the MTF systems, is willing to trust remote administrators, the systems they administer, or systems that may connect to the administrators' systems. Note that refusing to delegate trust does not mean that the agent is not trusted, it may be interpreted as the agent's trust model, i.e., who the agent trusts on their system, is either not acceptable or well understood.

**SYSTEMS ADMINISTRATION**

Systems Administrators are responsible for the permissions and services accorded to internal and external users. Their system configuration choices result in allowing or denying specific services to authorized users and to the outside world. These are critical decisions, and they may allow unintentional weakening of system boundaries both internally between systems as well as at the boundaries to the potentially malicious outside world. Because of the diversity and criticality of the systems administration functions, the area dealing with those functions are further broken into sections of observations and recommendations dealing with the critical components of the administrators' responsibilities.

***Systems Administration - Configuration***

Administration of system configurations addresses the services, software, and hardware used by user, server and application systems. The DHIAP team based their observations primarily on the technology review and interviews with the technical staff.

**MANAGEMENT OBJECTIVE:**

**All systems (NT servers, NT clients, Windows 95, Unix, and VMS) are configured with minimal services essential to supporting the mission requirements.**

***OBSERVATIONS:***

As delivered to and used by the MTF, configurations of many systems will not meet generally accepted security practices or DoD, Army, and MEDCOM regulations. Subjects where variances were found include: discretionary access control, auditing, auto-logout, world writeable user and system files, use of most restrictive permissions for file and directory access, password aging, account management, minimal services and applications, and running unnecessary services. Unnecessary TCP and UDP services were found to be running on several systems, and unnecessary services were found running on client NT workstations. Some services made system configuration or usage information publicly available, while other services could be used to gain unauthorized access to systems. Going beyond the officially procured MTF software, internal procedures currently are weak for evaluating the impact of the installation of non-standard software; there are no tools available to detect and track non-standard software and, because its installation is typically not coordinated with the IT staff, there is currently no way to evaluate the impact on the processing environment.

The preferred and generally accepted practice is to configure systems, whether internal or external, for the minimal set of system services that will support mission requirements. The challenge is to identify this minimal set without hampering operations. Issues that compound the challenge are diversity of systems and standards, remote administrators trying to determine a standard set of services that will not interfere with operations in a diverse number of sites, demands of critical system users for maximum flexibility, and the potential cross-system effects on interdependent systems. The seemingly safest routes for the harried administrator are either to defer the decision of system configurations to default settings or to

configure the systems as loosely as possible while keeping potential open holes in mind. These short-range tactics leave the systems open to exploitation. Vulnerabilities in default configurations are well known to malicious hackers and are often specific targets for penetration avenues. Adding to the complexity of deciding system and user configurations are the challenges of staying abreast of new potential exploitation methods as they emerge and of examining new features introduced by vendors to determine whether they introduce new vulnerabilities.

The recognized aid to system administrators is the configuration control board (CCB). The CCB provides a focus point and a decision body to work out acceptable system configurations. Generally they consist of managers and technical expert advisors. The DHIAP team found that CCB was in place but dealing at this detailed level of system configurations was not within their present scope. They are presently primarily involved in approving standard system hardware and software components.

***RECOMMENDATIONS:******Higher Echelons –Support for Computer Systems:***

1. Establish a command-level CCB to oversee system configuration guidance and decisions made on behalf of the Command.
2. Include Command CCB representation when making decisions about acquiring command wide computer systems.
3. Implement procedure for the Command CCB to work in concert with MTF CCBs in defining baseline configuration requirements for MTF systems, servers, and networks.

***MTF Management:***

1. Establish a CCB to review and approve MTF system decisions and plans. Include MTF management and MTF IT Group technical experts on the CCB to assure their work is based on comprehensive knowledge of the facility and its technical requirements.
2. Implement procedure for the CCB to: define baseline configuration requirements for MTF systems, servers, and networks; evaluate newly delivered systems for compliance with configuration requirements; and review/approve proposed system modifications. Assure that the MTF CCB coordinates its activities with the Command CCB where appropriate (e.g., for defining acceptable baseline configurations).
3. Evaluate the MTF's existing systems for compliance with standard security practice at the MTF and regulations of DoD, Army, and MEDCOM. Where deficiencies are found, take corrective action (e.g., fix the problem, inactivate the system, request exception to regulatory guidance, etc.).
4. Establish procedure to assure that the MTF's IT Group and CCB participate in approving, installing, and testing non-standard software at the MTF.

***IT Group Management:***

1. Configure systems for the minimal set of system services that will support mission requirements.

2. Acquire software-tracking tools to identify instances of non-standard software being installed and assure that appropriate staff is trained in their use.

**Systems Administration - System Services**

Systems Services include the basic configuration of services available to the user, standard interfaces for the operating system, and the configuration of certain key elements in the infrastructure such as the Domain Name Server, Simple Message Transfer Protocol, and network management tools. The DHIAP team reached their conclusions after analyzing the results of the external and internal network scans, the results of scripts run on each machine to capture its configuration, and one-on-one conversations with the technical staff.

**MANAGEMENT OBJECTIVE:**

**Systems are configured such that potential targets of exploitation are understood and vulnerabilities are minimized. System administrators and system managers have policies covering basic systems configurations, follow them, and are trained in the proper methods for configuring and securing systems.**

**OBSERVATIONS:**

Certain MTF system support practices expose the systems to risk. Perhaps most important, it is common practice for a single host to serve multiple purposes as the network management host, the primary DNS (Domain Name Service) host, and the SMTP (Simple Message Transfer Protocol) host instead of having these services isolated and rigorously secured from compromise. Some specific Observations in this area include the following:

- DNS configuration exposes internal systems: DNS has HINFO (Host Information) and WKS (Well Known Services) entries which provide information that can be used to attack the site. In addition, domain transfer is enabled, allowing the complete DNS table to be downloaded.
- There are a large number of world writeable directories and files on some systems.
- Permission settings are inadequately restrictive for many devices, files, and directories.
- The NT systems are often configured using the default settings rather than in accordance with accepted security practices. For example, some areas are not audited, audit logs are not protected from being automatically overwritten, and guest accounts and default administrator accounts are not renamed.
- Systems are typically delivered with limited or no audit capabilities, and systems personnel are not trained to implement such procedures for the systems they support.

Users who are untrained in systems administration carry responsibility for administration of the application systems. This practice exposes the MTF to risk as these users may be unaware of processes and procedures that would typically be enforced if trained technical staff were performing the responsibility

**RECOMMENDATIONS:**

**Higher Echelons –Support for Computer Systems:**

1. Oversee standards applied to system service configurations. Since many of these systems are centrally administered, it is incumbent on some expert oversight authority to ensure that the systems are configured in such a way so to minimize risk exposure.

**MTF Management:**

1. Assure that IT Group technical staff carries overall responsibility for administration of all MTF systems, including those directly maintained by outside organizations and/or by members of other MTF departments.
2. Assure that a principal from the MTF carries the responsibility to understand, monitor, and audit activity of each MTF system.

**IT Group Management:**

1. Define and implement department procedure to assure that MTF systems are in compliance with standard security practices and with DoD, Army, and MEDCOM regulations. Working with MTF Security Department, initiate appropriate remedial action and perform follow-up for all systems periodically to ensure continued compliance. Where remedial action is to be delayed or not taken, document and submit to MTF management a summary of the situation, the risks posed, and proposed resolution.
2. Acquire generally accepted automated tools to support the systems administration function (e.g., Windows NT's C2 Manager software) and assure that appropriate staff are trained in their use.

**Systems Administration - Network Operation and Services**

Network Operation and Services includes the operation of the network infrastructure and the services running on each user and application computer system. It also includes the user connectivity to the hospital via Internet Service Providers (ISPs), modem connection, and military sites. The DHIAP team reached their conclusions after analyzing the results of the external and internal network scans and the one-on-one conversations with the technical staff.

**MANAGEMENT OBJECTIVE:**

**Policy guidance is available and followed for: Internet usage for web, e-mail and data transfer functions; safe operation and maintenance of systems and software from remote locations; and hospital system access through Internet Service Providers, modem connections, and military sites.**

**OBSERVATIONS:**

Increasing dependency on the Internet for general communications and for performing work remotely introduces certain risks. The MTF have insufficient policies for use of the Internet, and users are not aware of the proper techniques and tools to use in their work. Non-secure, open communications without encryption or authentication/verification are normal, as there

is an erroneous assumption that private network security protects the access and transfer of sensitive information. Examples of sensitive information transferred in the clear include commands for remote system administration, user ids, and user passwords.

There are multiple unofficial access points to MTF systems and networks, both known and unknown, and limited availability of detailed documentation of the local network architecture makes it difficult to analyze threats. Systems are generally installed with default configurations, enabling unnecessary network services and therefore making these services accessible to the public. Firewalls have not been implemented, and only limited network logging and scanning tools are available for detecting instances of intrusion and analyzing networks and modems. System access requests are not authenticated on a consistent basis. In addition, methods used for external access via modem can put network and sensitive information at risk, as there is no use of such standard protections such as modem detection software, dial-back systems, or encryption of modem communications.

***RECOMMENDATIONS:******IT Group Management:***

1. Define procedures that outline safe techniques for accessing the Internet and performing work via Internet communications.
2. Document existing networks and establish a vulnerability profile for them. Implement fixes for identified problems. Evaluate use of firewalls to protect MTF network communications.
3. Acquire networking tools, modem tools, and intrusion detection tools and assure network administrators are trained in their use.
4. Incorporate modem detection software to identify unauthorized modems providing potential system back doors.
5. Implement strong user identification and authentication systems using such tools as dial back modems.
6. Consider encryption of modem communications to thwart interception of sensitive information on public networks and ISP.
7. Train users on safe use of the internet and automation tools such as e-mail to avoid security breaches from loading and launching applications or opening documents which may contain viruses.

***Systems Administration - Passwords and User Accounts***

The administration of password and user accounts includes user password selection and the issuing and termination of user accounts on all systems. The DHIAP team derived these observations from examination of procedures in use to administer accounts and interviews with members of the technical staff.



**MANAGEMENT OBJECTIVE:**

**Password and user account policies are in accordance with accepted security practices and ensure that only legitimate users can gain access to the systems and each user can only access systems and accounts for which he/she is authorized.**

**OBSERVATIONS:**

A system's users are identified and authenticated by a unique identification called a "user id." Its format typically follows an application standard such as first initial and last name. Used along with the unique identification is a secret password known only to the user and to the system. Creation of the password is normally a personal responsibility of the user, and it should always be a user's personal responsibility to remember the password in order to gain access to the system. Often, if given the opportunity, users will select passwords on the basis of how well they can recall the secret when needed. Satisfying that constraint often means that users pick weak, easy to guess passwords. Often, passwords are written down rather than committed to memory.

The DHIAP team observed that many users have multiple accounts, each with differing standards for assignment and maintenance of their passwords. This drives users to invent a single password for multiple systems, creating the weakness that discovering one password reveals all passwords. The team also heard reports of users sharing accounts and passwords to facilitate operational needs.

The MTFs do not have consistent procedures for reinitializing or changing passwords, or for inactivating user accounts at the time of a user's duty reassignment. MTF management of user accounts exposes system and patient information to unauthorized use, as indicated in the following observations:

- **Account Creation for New Users:** creating new user access profiles by copying from existing profiles may allow new users to "inherit" inappropriate permissions.
- **Account Update with Job Change:** MTF processes do not preclude individuals from retaining and accumulating account privileges when changing job functions. A user's access profile may be inappropriate for his or her current job function.
- **Account Termination:** MTF processes for termination of access are not consistently followed upon employee departure. Individuals who are no longer associated with an MTF may retain access to the MTF's data.

It should be noted that the potential for unauthorized access through "social engineering" was found where, in some cases, system access was granted without preliminary authentication of the request.

In some cases, access privileges were found to be overly permissive. Many accounts had the ability to override volume protection parameters and to change personal privileges. Some systems exhibited inadequate purging of accounts; many of these accounts had high level privileges, and non-existent users or groups owned many of the files and directories. There was no formal record of valid user groups and their members and no method of assuring that

purging of a terminated account included removal or archiving of its associated directories and files.

***RECOMMENDATIONS:***

***Higher Echelons – Support for Security Policy and Procedures:***

1. Develop command wide standards for password creation, administration, and use that applies to all systems.
2. Investigate use of technologies that support using a single sign-on to gain access to multiple independent systems.

***MTF Management:***

1. Define policy for user access to MTF systems that requires single-user, confidential passwords and limiting access to the functions required to perform assigned work. Policy should include:
  - Outline requirements for related issues such as confidentiality of the password (backed up by user signed acceptance of the policy);
  - regular change of passwords based on elapsed time;
  - change of passwords and privileges based on duty reassignment; and
  - deletion of access privileges/passwords based on duty reassignment/termination.
2. Establish procedure for documenting management approval of requests for user access to systems.
3. Establish procedure for the MTF to automatically provide IT notification of users' job status changes and for IT to re-evaluate/update user access privileges in a manner appropriate to the status change.

***IT Group Management:***

1. Establish procedure for management of user passwords and access privileges. Include user-friendly, secure processes for: establishing new user access privileges/password, changing access privileges/passwords, evaluation of requested passwords against criteria defined to prevent use of "simple" character combinations.
2. Obtain appropriate authority to run password-checking tools on all systems to identify flagrant violation of password security practices.
3. Investigate and resolve user access/password issues from the past, including existence of superfluous accounts, files/directories owned by terminated or superfluous accounts, and accounts established for groups of users.

**TRAINING**

The training examined here is limited to security training of end users, technical staff, and security managers and technical training of the IMF staff. User knowledge of the operation of the equipment and software, outside of security procedures, is not within the scope of this item. The DHIAP team reached these conclusions after examining training material and interviewing members of the staff.

**MANAGEMENT OBJECTIVE:**

**Individuals have knowledge of security practices sufficient to support secure operation of the site's systems and applications. Security managers and technical staff have technical foundation in security principles sufficient to apply acceptable security practices to normal operations.**

***OBSERVATIONS:***

Technology is evolving rapidly, and the effect of that rapid evolution is magnified by the complexity of the emerging technology. The challenge is often how to maintain technical proficiency. The technical staff at the sites visited have done a remarkable job in assimilating new technologies in networking, client-server architectures, Internet communications, and a myriad of function-specific systems. The emerging challenge will be to build and maintain proficiency in the area of securing systems.

At the time of the DHIAP evaluation, security training for technical staff, users, and individuals responsible for implementing or assuring compliance with security functions was incomplete. The technical staff security training and experience did not include training on security practices for specific hardware platforms, and introduction of new systems to an MTF included little or no training on new equipment. Although it is important for IT Group knowledge of information security threats and practices to be refreshed frequently, updates on emerging/current information security threats, actual cases, safe practices, Internet, and the Web are rarely provided by higher level command.

Users need not only awareness of security issues, but sufficient understanding that they can make a sound decision when faced with alternatives. The users' orientation briefing does not clearly enable users to understand security issues as they relate to their jobs. Many users receive no security training other than the CHCS security module, based on an assumption that the user carries over the CHCS training to other systems. However, it was observed that users do not consistently exercise fundamental information security practices. Managers need appropriate level of expertise in this area to evaluate the risks, assess the resources needed to mitigate those risks, and make the decisions on which risks to accept and which to resolve. There is little ongoing training (e.g., orientation briefing, refresher training, Computer Based Training, etc.) to provide updated, specific security guidance to users, and there is no measure of the effectiveness of orientation and annual training.

**RECOMMENDATIONS:**

**Higher Echelons – Support for Security Policy and Procedures:**

1. Identify a central source of security awareness training and develop for distribution information suitable for adaptation at the MTF level on safe security procedures, security threats, and actual cases.

**Higher Echelons –Support for Computer Systems:**

1. Require managers of centralized system to include security training component for new equipment training as appropriate.

**MTF Management:**

1. Assure that MTF staff is provided with security training appropriate to their organization role when they join the facility, and that training updates/refresher training is provided on a regular basis. Incorporate information assurance training in to manager development training.
2. Assure that appropriate MTF staff are provided with training on safe techniques for accessing the Internet and performing work via Internet communications.
3. Implement methods for monitoring effectiveness of security training and staff members' consistency in exercising fundamental information security practices.

**MTF Security Department Management:**

1. Assure that MTF orientation training for staff/employees in new positions includes training on security issues that relate to the staff members' new jobs.
2. Develop and provide general security training for all users.
3. Develop and provide security training appropriate for each MTF system, for the users of that system, and for its IT support staff.
4. Assign at least one individual to develop expertise in security with special focus on the site's dominant systems.

**IT Group Management:**

1. Provide detailed technical training on security practices for specific computer platforms to appropriate IT staff. Regularly provide updated training/refresher training.
2. Increase staff and user awareness of security issues by providing information regarding current information security threats, actual cases, and safe practices.
3. Provide IT staff training on safe techniques for accessing the Internet and performing work via Internet communications.

**DISASTER RECOVERY AND SYSTEM BACKUPS**

The area of Disaster Recovery and System Backups is defined as prevention of loss of system access and data and timely restoration of services in case of failure. It includes single user/patient data loss and loss of system and/or data access. The DHIAP team reviewed disaster recovery policies, visited computer areas, and conducted one-on-one interviews with the technical staff.

**MANAGEMENT OBJECTIVE:**

**Information assurance policies and procedures are sufficient to assure that full recovery occurs in a manner and timeframe that permits unimpeded operation of the facility.**

***OBSERVATIONS:***

The DHIAP team noted that disaster planning and recovery was present at each site visited, but also identified areas where the planning could be improved. MTF system backups and disaster recovery plans are inadequate to reliably restore all system operations and data. In some circumstances, even minor problems will result in loss of system operation and data. Plans for Disaster Recovery are incomplete and out of date, not covering all applications and servers and common cause failures could lead to both systems and backups being lost in the same events.

Backups, an essential component for recovering from disaster, are not consistently performed for all clinic and server systems. Procedures for retention/rotation of backup media are not sufficient to support restoration of the systems; on many systems the backup media are recycled in less than a month. The "offsite" locations where backups are stored are often subject to damage by the same disaster that might strike the production computing environment. In one situation, the team noted that a single point of failure (a broken tape drive unit) prevented performance of system backups.

Protection from disasters occurring within the computers' physical environment is less than adequate. Fire suppression in some critical computer rooms is water-based, establishing a potential for shock hazard and loss of equipment. Uninterruptible Power Supply (UPS) units are not adequately sized to operate during extended outages, and the older batteries used in UPS units might not be sufficient to allow a controlled power shutdown.

***RECOMMENDATIONS:***

***MTF Management:***

1. Work with MTF Security Department and IT Group management to prioritize system resources for coverage by the MTF's Disaster Recovery Plan
2. Assure that Disaster Recovery Plans in effect for the facility's computer systems are adequate.

**IT Group Management:**

1. Review and update the MTF's Disaster Recovery Plan, ensuring it adequately covers the current portfolio of systems and the current physical configuration of the MTF facility. Verify adequacy of retention and storage location for backup media.
2. With Security Department, verify that IT backup/recovery procedure is properly coordinated with user departments' procedures for reestablishing processing capability following a disaster (e.g., paper documents needed to carry operation forward from time of last backup are available for use).
3. Assure all backup/recovery hardware is in place, sufficient to meet current demand, and operating properly.
4. Test backup/recovery procedure for every MTF system and ensure that no single point of failure will result in the inability to backup/recover information and software.
5. Include inspection and evaluation of computer room environment, including: fire suppression, cooling, UPS sizing and UPS battery maintenance in disaster recovery planning.

**PHYSICAL SECURITY**

Physical security is defined as the protection of computer and network systems, patient records, and individuals from harm, damage, injury and loss. The DHIAP team reached the conclusions which follow from observing standard practices while on-site at the MTF and through discussions and interviews with MTF staff.

**MANAGEMENT OBJECTIVE:**

**Physical Security policies and procedures are understood, practiced, and verified. Individuals understand and follow the policies and procedures well enough that detection of a violation is immediately noticed, reported to the appropriate authority, and acted upon without delay.**

***OBSERVATIONS:***

While not the main focus of this effort, physical security can be a significant risk for loss of control over sensitive information. Losing an asset such as a workstation is not only a loss of the physical asset but also a potential exposure of any stored information. Loss does not have to be something as visible as a workstation; it can also be something as concealable and reusable as magnetic media. Physical security includes not only what may be taken from the area but what can be inserted into the area, for example, a cable sniffing device to eavesdrop on sensitive information inside an assumed closed environment.

Some elements of physical security at the MTF site are inconsistently practiced, jeopardizing information and personal security. In some cases, buildings are open to the public 24 hours a day and in other cases, building security may be easily breached (e.g., through back and side doors that are propped open for convenience). In each case, patient floors and clinics, and the computing equipment located there, are accessible to unauthorized individuals. There are some reports of missing computer equipment. It was reported as difficult to identify or track the missing equipment because property control records are insufficient. Lost with the equipment are any data records stored on the devices.

Another form of physical security is the treatment of the paper and media where confidential information (both patient information and materials marked "for official use only") is recorded. In many instances confidential information is not destroyed immediately after use; because destruction of patient records is not convenient, the situation worsens as hardcopy patient records accumulate.

***RECOMMENDATIONS:******MTF Management:***

1. Define a physical security policy, and define/enforce procedures to assure physical security of patient information used at the MTF.
2. Reinforce property control procedures with spot checks of inventory locations (e.g., terminal areas, patient floors, etc.).
3. Evaluate the need for limiting access to each area of the MTF (e.g., records rooms, terminal areas, patient floors, etc.) and install control devices that are appropriate to the

situation (e.g., lock and key, combination code locks, badged entry devices, cameras/monitors/staffing, etc.).

4. Identify areas of the MTF where paper copies of sensitive patient data and materials marked "for official use only" are discarded (e.g., physician offices, clinics, registration areas); install devices (e.g., paper shredders) or implement procedure (e.g., deposit in specially colored trash bins that are periodically emptied/contents shredded) to ensure the paper is disposed of properly and in a timely manner.
5. Train MTF staff on physical security policy and procedures; retrain staff as changes are made. Incorporate physical security training into the annual training refresher program.
6. Perform periodic audits of compliance with physical security procedure and policy, report and act on violations, define recommendations for updating procedure and policy as the environment changes.





DEPARTMENT OF THE ARMY  
US ARMY MEDICAL RESEARCH AND MATERIEL COMMAND  
504 SCOTT STREET  
FORT DETRICK, MARYLAND 21702-5012

REPLY TO  
ATTENTION OF:

MCMR-RMI-S (70-1y)

5 Jun 02

MEMORANDUM FOR Administrator, Defense Technical Information  
Center (DTIC-OCA), 8725 John J. Kingman Road, Fort Belvoir,  
VA 22060-6218

SUBJECT: Request Change in Distribution Statement

1. The U.S. Army Medical Research and Materiel Command has reexamined the need for the limitation assigned to technical reports written for Grant DAMD17-99-C-9001. Request the limited distribution statement for Accession Document Number ADB263640 be changed to "Approved for public release; distribution unlimited." This report should be released to the National Technical Information Service.

2. Point of contact for this request is Ms. Judy Pawlus at DSN 343-7322 or by e-mail at judy.pawlus@det.amedd.army.mil.

FOR THE COMMANDER:

A handwritten signature in black ink, appearing to read "Phyllis M. Rinehart".

PHYLLIS M. RINEHART  
Deputy Chief of Staff for  
Information Management