NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CYBERCIEGE CAMPAIGN FULFILLING NAVY INFORMATION ASSURANCE TRAINING AND AWARENESS REQUIREMENTS

by

Benjamin D. Cone

March 2006

Thesis Advisor:	Cynthia Irvine
Second Reader:	Nelson Irvine

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

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 instruction, 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** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: A CYBERCIEGE Campaign Fulfilling Navy Information Assurance Training and Awareness Requirements		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Benjamin D. Cone			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The broad use of information systems within organizations has led to an increased appreciation of the need to ensure that all users be aware of basic concepts in Information Assurance (IA). The Department of Defense (DOD) addressed the idea of user awareness in DOD Directive 8750.1. This directive requires that all users of DOD information systems undergo an initial IA awareness orientation followed by annual refresher instruction.

This thesis created a CyberCIEGE campaign for the Naval Postgraduate School's CyberCIEGE project that will fulfill Navy requirements to meet DOD Directive 8750.1. The first portion of this thesis is an analysis of four IA programs and products. Requirements for Navy IA awareness and training products were developed from this analysis. The second part of this thesis is a description of two CyberCIEGE scenarios that were created to fulfill these requirements. The first scenario focuses on basic IA awareness and emphasizes information that the Navy should reinforce. The scenario is intended for all users of Navy information systems. The second scenario is intended for technical users and addresses more advanced concepts and technical considerations. The technical user scenario emphasizes skill application and problem solving.

14. SUBJECT TERMS CyberCIEGE, Information Assurance, Training, Awareness, DOD Directive 8750.1, Computer Security			**15. NUMBER OF PAGES** 280
			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** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A CYBERCIEGE CAMPAIGN FULFILLING NAVY INFORMATION ASSURANCE TRAINING AND AWARENESS REQUIREMENTS

Benjamin D. Cone
Lieutenant, United States Naval Reserve
B.S., United States Naval Academy, 1998

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2006**

Author: Benjamin D. Cone

Approved by: Dr. Cynthia Irvine
Thesis Advisor

Dr. Nelson Irvine
Second Reader/Co-Advisor

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The broad use of information systems within organizations has led to an increased appreciation of the need to ensure that all users be aware of basic concepts in Information Assurance (IA). The Department of Defense (DOD) addressed the idea of user awareness in DOD Directive 8750.1. This directive requires that all users of DOD information systems undergo an initial IA awareness orientation followed by annual refresher instruction.

This thesis created a CyberCIEGE campaign for the Naval Postgraduate School's CyberCIEGE project that will fulfill Navy requirements to meet DOD Directive 8750.1. The first portion of this thesis is an analysis of four IA programs and products. Requirements for Navy IA awareness and training products were developed from this analysis. The second part of this thesis is a description of two CyberCIEGE scenarios that were created to fulfill these requirements. The first scenario focuses on basic IA awareness and emphasizes information that the Navy should reinforce. The scenario is intended for all users of Navy information systems. The second scenario is intended for technical users and addresses more advanced concepts and technical considerations. The technical user scenario emphasizes skill application and problem solving.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge and thank those who dedicated their time and support for me during the thesis process. First and foremost, I would like to thank my wife, Collene and my son, Jack. Without your support, I would not have been able to do well here. Second, I would like to thank Mike Thompson. Thank you for your consistent patience in answering my questions about CyberCIEGE. Third, I would like to thank my thesis advisers, Drs. Cynthia and Nelson Irvine. I really appreciated your quick feedback and guidance. Although the amount of feedback was humbling at times, I really appreciated it and learned a lot from you during the thesis process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

A. PURPOSE

The purpose of this thesis is to create a CyberCIEGE campaign for the Naval Postgraduate School's CyberCIEGE project that will fulfill U.S. Navy requirements for annual Information Assurance (IA) awareness in accordance with Department of Defense (DOD) Directive 8570.1. The directive requires that all authorized users of DOD systems undergo an initial IA awareness orientation and annual IA refresher awareness [DOD 2004]. CyberCIEGE is a training tool that may aid Navy organizations in fulfilling their obligations under this DOD directive.

B. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) IT SECURITY LEARNING CONTINUUM

[NIST1 1998] presents the IT Security Learning Continuum as a model for learning in IT Security. This model identifies three levels of learning and is illustrated in Figure 1. The first level is awareness. Awareness serves to focus attention of all IT users on IT security. According to [NIST1 1998], the objective of awareness is recognition and retention of information. This is the level of learning addressed in DOD Directive 8750.1. The second level in the continuum is training. The training level focuses on producing security skills for those who have roles and responsibilities relative to IT systems. The highest level is education. The education level focuses on understanding a common body of knowledge with respect to IT security. The NIST model assumes that learning is a continuum and learning "starts with awareness, builds into training, and evolves into education." This thesis will focus on awareness and training, and will not address education.

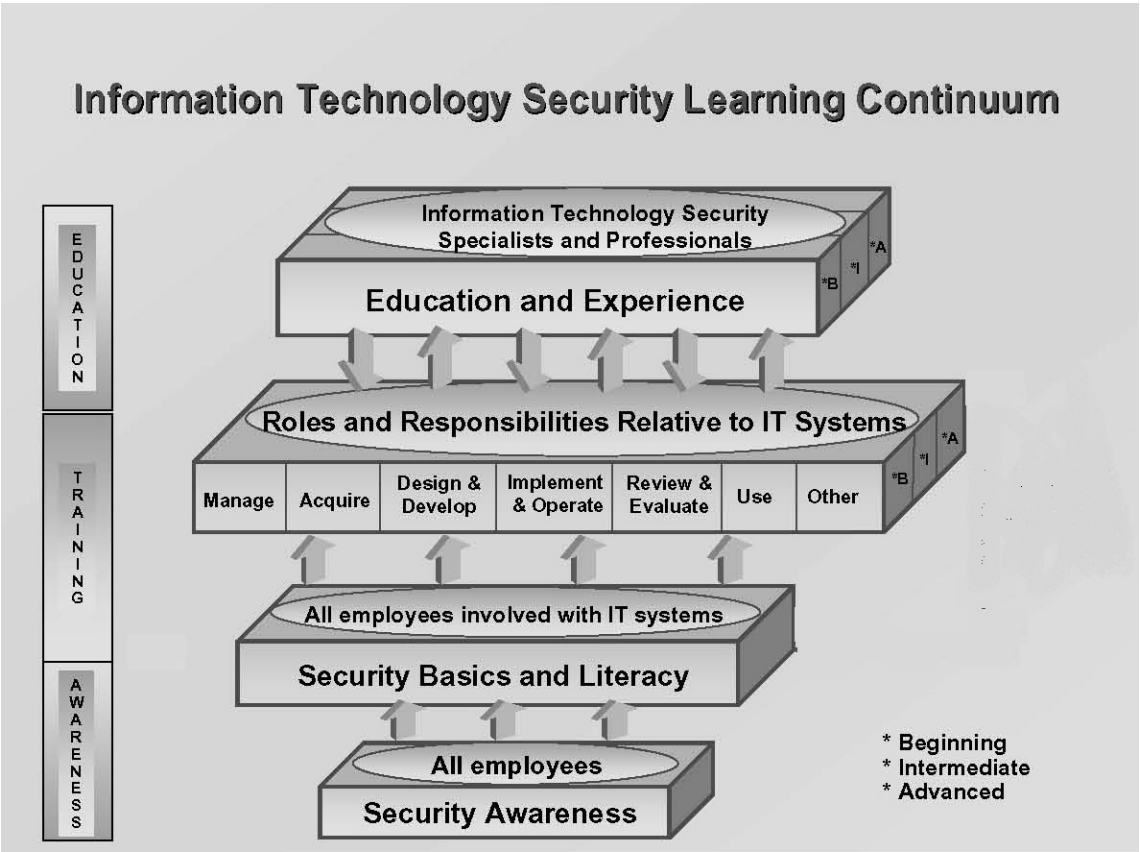

Figure 1. NIST IT Security Learning Continuum (From [NIST1 1998])

C. EVOLUTION OF NAVY TRAINING AND AWARENESS POLICY

The Navy Information Security Program regulation places the burden of responsibility of security education upon individual unit Commanding Officers [Navy1 1999]. This regulation does not distinguish between different levels of learning. Traditionally, the implementation of information security training and awareness is delegated to each local Information Systems Security Manager (ISSM) [NAVSO1 1995]. The ISSM is responsible for developing local training sessions or Computer-Based Training (CBT) in order to fulfill the requirement for periodic training. From a Navy-wide perspective, this represents a decentralized approach to the IA training and awareness problem. This approach to training and awareness allows the organization the liberty to tailor its training to a local context at the expense of uniformity across the enterprise. Since the mid 1990's,

the focus of training and awareness has slowly evolved to a more centralized approach as reflected in the enactment of Federal legislation and DOD Policy.

The Federal Information Security Management Act of 2002 provided further guidance on Federal agency training and awareness programs. This act mandates that Federal agencies shall conduct periodic security training that focus on information security risks and the responsibilities of all personnel, including contractors, to comply with agency risk reduction policy and procedures [FISMA 2002].

In August 2004, the Department of Defense issued DOD Directive 8570.1 which mandated that all DOD Information System users undergo initial Information Assurance training followed by annual refresher training. The issuance of this directive has highlighted the importance of fostering a security culture and the need to find training techniques that will actively engage the typical user. Since this directive, all users of Navy information systems have been instructed to complete the DOD IA Awareness Computer-based Training (CBT) [DISA 2004]. While local ISSM's still have authority to conduct additional training on local procedures and policy, the DOD IA Awareness CBT serves as a baseline level of standardization to which all Navy personnel must be trained.

D. COMMON TECHNIQUES FOR TRAINING AND AWARENESS

NIST Special Publication 800-50 [NIST2 2003] lists several techniques for training and awareness dissemination, but most of these techniques can generally be categorized into one of four distinct groups.

1. Formal Training Sessions

Formal Training Sessions can be conducting in a variety of ways. They can be instructor-led, "brown-bag" seminars, or video sessions. Formal training sessions facilitated by local information security personnel represent the traditional approach to user training and awareness within the Department of the Navy. This technique offers the flexibility to tailor training sessions to address

locally-relevant security issues and provide hand's-on demonstration of security mechanisms. The flexibility of this approach offers a good "fit" to the security posture of the local organization. The flexibility of this approach to address locally-relevant issues can be limited by upper-management policy regarding the content of the training in order to establish enterprise-wide baseline training. Disadvantages to this approach include the expense of tailoring facilitator-led training and the inconvenience of scheduling training during business hours. The success of this approach often depends upon the ability of the training facilitator to engage the audience and upon local management to provide support for this training.

2. Computer and Web-based Training

Computer-based and web-based training represents a centralized approach to the training and awareness problem. Computer-based training offers users the flexibility to complete training at their own pace and the organization the ability to train users to an enterprise-wide standard at lower cost and higher convenience. The disadvantage of this technique is that training and awareness becomes a passive exercise that does not challenge the user or provide a dialogue for further discussion. CBT becomes merely something that the user must complete with minimal impact upon the user's schedule. Often, self-paced CBT can be undermined by simply skipping or rapidly clicking through slides. The success of this technique lies in the ability of the CBT developer to provide an engaging course of instruction within the constraints of training requirements.

3. Awareness Messages

This technique seeks to raise the level of awareness through the delivery of awareness messages in the workplace. Some of the more common methods of delivery include organizational newsletters and memos, email messages, posters, and security labels. This approach is common in the Department of the Navy and serves to provide another layer of awareness to the user in the

workplace. This approach is a passive technique that serves to reinforce awareness lessons learned from other sources. The major benefit of this technique is that awareness messages are integrated into the workplace.

4. Video Games

Video games represent a completely different approach to training and awareness. This technique seeks to engage a user community through a gaming experience. Unlike the other techniques, video games offer an active approach to training and awareness by placing the burden of responsibility for decision-making on the user. By creating a virtual world, a game player can be introduced to concepts and ideas that the user may not realize are a part of their real jobs. In a video game, a player can learn about the security ramifications of decisions they make without the actual degradation of the organizational security posture. Scenario-based video games also offer the flexibility of communicating specific targeted messages or enterprise-wide security goals. The CyberCIEGE video game falls into this category and offers the advantage of providing a training and awareness vehicle that can be customized to a specific user group's requirements.

E. CYBERCIEGE BACKGROUND

CyberCIEGE is a video game for teaching Information Assurance concepts and principles. CyberCIEGE was developed at the Naval Postgraduate School in partnership with Rivermind, Inc. Based upon popular commercial video games, CyberCIEGE allows the player to assume the role of a decision-maker within an organization. In this role, the game-player must make decisions in a manner that minimizes vulnerabilities while ensuring workplace productivity by allowing users (game characters) to accomplish their goals (known as asset goals in the game). The player must manage risk by protecting assets from potential attackers while ensuring that users can access their assigned assets.

The CyberCIEGE game consists of several components: a simulation engine, Scenario Definition Tool (SDT), Scenario Definition Language, Campaign Analyzer, and game encyclopedia. Scenarios can be built in the SDT using the CyberCIEGE- specific Scenario Definition Language. Figure 2 displays the SDT. Scenarios can be tailored for a particular user community with specific training requirements [Irvine2005].

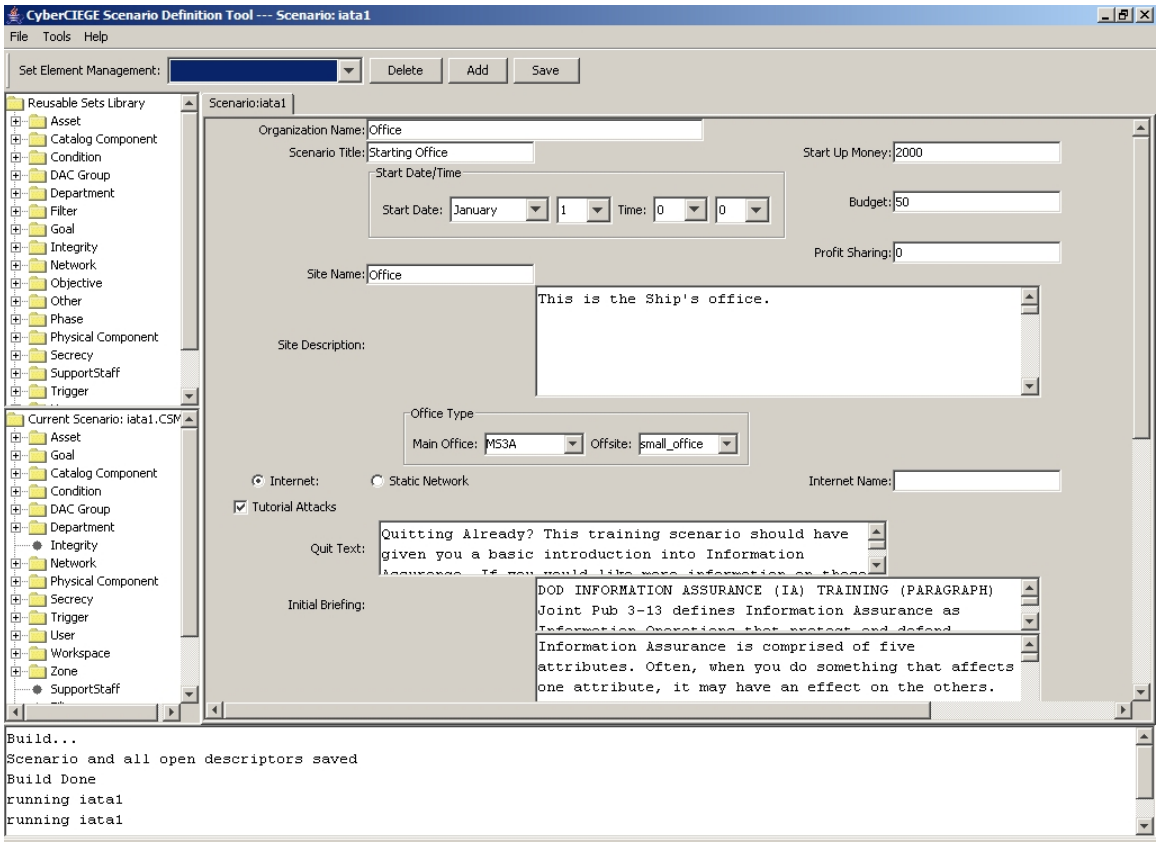

Figure 2. Scenario Definition Tool

A typical scenario begins with an initial briefing that provides the opening context for the scenario and the overall objective to the player. After the initial briefing, the player is brought to the three dimensional game playing screen. From the main game playing screen, a scenario may be played out in a variety of

ways. Typically, a player will have to achieve specific objectives to progress through the game, although this is scenario specific.

Once a scenario begins, game players can navigate through various screens by clicking on different tabs in order to accomplish their objectives. The office tab is the first game screen that the player sees. From this screen, the player can observe the simulation from a three dimensional perspective. Figure 3 is a graphical representation of this screen. The player can pause the game or view the objectives for the game in the office tab. The network tab allows the player to build, change, or configure the computer networks in the game. The component tab allows the player to configure individual components in the game. The zone tab allows the player to configure smaller areas of the workspace. The user tab provides information on individual game characters, their status in the game, and gives the player the ability to purchase training for the characters. The asset tab allows the player to view information on the information assets that must be protected in the game. The game tab allows the player to view the initial briefing as well as view the various discretionary and mandatory access control groups defined in the scenario.

Figure 3. CyberCIEGE Office Screen

F. RESEARCH QUESTIONS

This thesis seeks to determine whether CyberCIEGE can be used to satisfy the requirements for annual IA awareness and training instruction in the Navy. To determine this, several research questions need to be answered. First, what are the Navy requirements for IA awareness and training? This question will be answered by researching the various policies and programs concerning Information Assurance training as well as analyzing past and current training and awareness products within the Federal government. A list of requirements will be generated in the requirements analysis portion of this thesis.

Second, how can CyberCIEGE use fulfill Information Assurance awareness and training requirements? This question will be answered by

analyzing the Navy requirements generated from the requirements analysis portion of this thesis. Ultimately, CyberCIEGE scenarios will be created in order to fulfill the specific requirements developed in the requirements analysis.

Third, can CyberCIEGE be tailored to a large organization with different levels of system user expertise? This question seeks to determine if an enterprise-wide awareness and training scenario is sufficient to raise awareness among users with various levels of system access. The answer to this question will determine if it is appropriate to develop more than one scenario for annual awareness and training for different levels of users.

G. METHODOLOGY

This thesis includes a literature review of possible sources of IA training and awareness requirements. Sources will include Federal law, Federal publications, and DOD policy and publications. Initial requirements will be extracted from current and past DOD training material as well as regulatory guidance. These requirements will be compared with NIST guidelines for building an IT security training and awareness program in order to ensure that relevant topics are covered. IA education as defined by NIST will not be addressed. Appropriate CyberCIEGE scenarios will be created addressing these requirements.

H. THESIS ORGANIZATION

This thesis is organized into five chapters. Chapter II is an analysis of current and past IA awareness and training products and compares various requirements with NIST documentation. Specific requirements for an IA awareness program within the context of the Department of the Navy are discussed.

Chapter III is a description of the basic user CyberCIEGE scenario that was created as part of the proposed solution for a CyberCIEGE campaign for Navy IA awareness.

Chapter IV is the description of the technical user scenario that was created as part of the proposed solution for a CyberCIEGE campaign for the Navy.

Chapter V consists of IA awareness and training scenario development concerns, recommendations for further study, and conclusions developed in this thesis process.

I. EXPECTED BENEFITS OF THIS THESIS

This thesis addresses those topics that should be covered in an IA training and awareness program for various U.S. Navy organizations. Chapter II can serve as a guide for training and awareness implementers in the determination of the topics that should be addressed in training and awareness programs.

Additionally, this thesis displays the flexibility of the CyberCIEGE project. Requirements for a specific user community were developed and CyberCIEGE was tailored to fulfill those requirements. The scenarios created from this thesis can be used in Navy IA training and awareness programs.

II. NAVY INFORMATION ASSURANCE (IA) TRAINING AND AWARENESS REQUIREMENTS ANALYSIS

A. TOPICAL REQUIREMENTS DISCOVERY

Two IA programs and two IA awareness and training products were analyzed in order to determine topical requirements for a Navy-wide IT security awareness product. The legacy Navy INFOSEC program and NIST SP 800-50 were analyzed to understand broad IA program-level requirements. Although dated, the Navy INFOSEC program provides guidance for IA awareness and training programs within the context of the DON. NIST SP 800-50 provides guidance for building an IA awareness program in accordance with Federal guidelines. Two specific IA products were analyzed in order to understand current trends in IA awareness and training requirements within the DOD. The DISA Computer-based Training provides a DOD enterprise-wide view of a specific IA training and awareness product. The DISA awareness briefing provides a current view of IA concerns within the context of a single organization.

1. Navy INFOSEC Program

Legacy Navy requirements for user information security training are found in the Navy INFOSEC program guidebooks for local Information System Security Officers (ISSOs), Information Security System Managers (ISSMs), and Network Security Officers (NSOs) [NAVSO1 1995, NAVSO2 1996, and NAVSO3 1996]. These documents offer recommended training curriculum topics and subtopics that training sessions may address. Table 1 consolidates and summarizes the topics that these documents recommend for an information system or network security training briefing.

- **Value of information**
  - Historical data
  - Personnel files, payroll data, legal records
  - Trade secrets or proprietary data
  - Documentation vital to national security
- **Password management**
  - Generation of unique passwords
  - Password protection
  - Changing passwords
- **Command specific security procedures**
  - Use of security products (safes, cipher locks, burn bags, classified disks)
  - Relocation of system and network components
  - Changing system and network software and hardware
  - Reporting actual or suspected security violations
  - Using networked games, homepages, shared files, etc
- **Communication and computer vulnerabilities**
  - Human errors
  - Misuse of the system (procedures not followed, data used for illegal purposes, "browsing", etc.)
  - Computer viruses
  - Internet security risks
  - Unauthorized use (e.g. hackers using network to steal information)
  - Natural hazards (fire, smoke, static electricity, extreme temperatures, humidity magnetic forces)
- **Virus prevention and detection**
- **Explanation and demonstration of security mechanisms and safeguards of the Information System**
- **Importance of self monitoring-Identification of successful and unsuccessful logons**
- **Importance of being alert to suspicious and unusual activity**
- **Current telecommunications security issues (encryption, network vulnerabilities inherent to various network components)**
- **Basic safe computing**
  - Maintenance of established network configurations
  - Accessing data (least privilege)
  - Warning banners and screens
  - Using keyboard or system locks
  - Unattended computers
  - Data destruction and disposal
  - Using, handling, and explanation of classified or sensitive data
  - Explanation of the differences between classified and unclassified networks
  - Backups
  - Use of unauthorized software
  - Protection of software
  - Use of modems
  - Interface awareness

Table 1. Consolidated List of Awareness and Training Topics From NAVSO Series Documents (After [NAVSO1 1995, NAVSO2 1996, and NAVSO3 1996])

2. NIST SP 800-50

NIST Special Publication 800-50 provides guidance for building an Information Technology Security training and awareness program. This document was published in October 2003 and standardizes many of the topics that were addressed in the Navy INFOSEC program. This document provides a thorough list of potential IA awareness and training topics which are summarized in Table 2.

• Password issues
  o Creation
  o Changing
  o Protecting
• Protection from malicious software
• Policy and implications of non-compliance
• Unknown email attachments
• Web usage and monitoring
• Spam
• Data Backup and storage
• Social engineering
• Incident response contacts
• Shoulder surfing
	• System or environment change
	• Inventory and property transfer
	• Personal use and gain issues
	• Handheld device issues
	• Use of encryption
	• Laptop security on travel
	• Personally owned systems at work
	• System patching and Configuration management
	• Software license restriction issues
		• Individual accountability
		• Use of acknowledgement statements
		• Visitor control and physical access to spaces
		• Desktop security
		• Information protection and confidentiality concerns
		• Email list etiquette-file attachments
		• Access control issues

Table 2. IA Awareness and Training Topics From NIST SP 800-50 (After [NIST2 2003])

3. DISA DOD IA Training CBT Version 2.0

The majority of naval organizations currently use the "DOD Information Assurance Awareness" CBT to fulfill their obligations for annual refresher training for Information System users. The training can be completed online as Web-based training or it can be completed offline as a CBT. This product is overtly outcome-based and explicitly addresses training objectives for the user. This product presents information from a DOD-wide perspective and addresses many common IA concerns. The major benefit of this training is that it establishes a baseline level of training for all personnel. The disadvantage of this training product is that it cannot address additional information on locally-relevant issues nor does it provide points for which personnel may want further elaboration. This training is broken up in modules and is summarized in Table 3.

- Course Overview and Objectives
- Importance of IA
  - Introduction
  - IA Overview
  - Evolution of IA
  - 'Policy and Law
  - Critical Infrastructure Protection Program
  - Conclusion
- Threats to IA
  - Intro
  - Threats and Vulnerabilities
  - Social Engineering
  - Internet Security
  - Conclusion
- Malicious Code
  - Intro
  - Malicious Code Overview
  - Understanding Internet Hoaxes
  - Conclusion
- User Roles
  - Intro
  - System Security
  - Protecting DOD Information
  - Conclusion
- Personal and Home Computer Security
  - Intro
  - Online Transactions
  - Security Tips
  - Conclusion

Table 3. Summary of Topics From DISA CBT (After [DISA1 2004])

4. DISA Information Assurance Security Awareness Briefing

The Defense Information Systems Agency has made an internal IA awareness briefing available on the Internet. This product reflects the perspective of a smaller organization. It includes many topics that the other products address as well as specific topics that the other products do not. The major benefit of this training product is that it illustrates many of the current IA concerns that DISA has deemed to be important. Table 4 summarizes the topics in this product.

• User responsibility • Login Banner • Definitions • Importance of IA training • Peer-to-peer risks, dangers, and policy. • Workstation Security: strong passwords, lock when leaving, Common Access Cards (CAC) to digitally sign and encrypt email • Handling, destruction, and storage of classified information	• Duties for personal and government equipment: don't process government information on personal computers, don't attach personal wireless devices to government networks, turn off phones and PDAs in classified areas, use encryption with wireless equipment, disable wireless cards when computer plugged into network, turn off wireless in classified areas • DOD commercial wireless devices policy • Definition of information • Levels of classification • Reporting security incidents and suspicious activity • Network security and internet practices: use caution when opening suspicious emails, organizational email use policy, virus protection	• Protection of computerized equipment: o Information at rest, labels, fundamentals of labeling o Information in transit: spillage, cost of recovery and why it occurs, o Processing information: controlled areas for classified material, removable hard drives, keep monitor turned away from open doors and windows

Table 4. DISA Awareness Brief (After [DISA2 2005])

5. Comparison of Training and Awareness Products and Programs

The Navy INFOSEC program represents a decentralized approach to IA awareness and training. In this program, local security personnel have been given the responsibility for analyzing and addressing IA awareness and training issues for the local organization. Although dated, the program documentation serves as a useful guide in determining Navy-relevant awareness topics.

NIST SP 800-50 provides a standardized approach for building an IA awareness and training program. NIST SP 800-50 takes a more thorough approach than the other programs and products investigated here since it provides guidance for building a program from a generic system perspective. The topics presented in NIST SP 800-50 are relevant in that they address issues that occur in many different types of organizational systems.

The DISA DOD CBT is a specific product that introduces Information Assurance concepts and principles to the user. This training has to remain somewhat generalized in that its recipients operate in many different DOD organizations. The major benefit of this product is that it breaks down the training into various sections which focus on individual topic areas such as the importance of IA, various threats to IA, and explaining user roles.

The DISA Awareness Brief represents an analytical approach similar to that advocated by the Navy INFOSEC program. This training product addresses many universal issues relevant to IA awareness, including basic definitions of Information Assurance concepts. This product also addresses many current challenges to IA in the DISA organization, including wireless devices, peer-to-peer issues, and organizational procedures. This product provides the training recipient with an explanation of the necessity of the training, but does not communicate what the outcomes of the training should be.

The contents of these products and programs were written over a period of a decade. This was during a time of rapid growth and evolution with respect to IT. While the importance of some topics such as password protection has not changed over this period, others have. For instance, the NAVSO 5239 series identifies payroll records as valuable information that must be protected. While this is still true, the DOD currently processes payroll information in a centralized manner and predominantly disseminates this information to individuals over the Internet. Individuals can logon to their Defense Finance and Accounting Service (DFAS) account and view their pay information from any computer terminal connected to the Internet. In this environment, protecting payroll information has almost become a non-issue for most naval organizations for reasons described below. The NAVSO 5239 series documents were written during a time when payroll documents such as Leave and Earning Statements (LES) were distributed in the workplace twice a month. Currently, it is becoming increasingly difficult to find paper copies of a LES within the boundaries of most Navy organizations. In fact, most of these organizations don't even have access to the payroll data for their personnel. However, the NAVSO 5239 series documents

are valuable in that they do identify some Navy-specific issues that transcend the evolution of IT. Topics such as information value determination fall into this category. NIST SP 800-50 adds value in that it provides a relatively current and thorough list of IA awareness and training topics. Even though they are not exhaustive, the DISA CBT and IA Awareness Briefing are valuable in that they highlight current topics of importance to IA. The DISA CBT in particular does a good job in presenting a framework for understanding IA concepts, although at the expense of providing an interactive environment where the user can actively learn and apply IA concepts.

Table 5 provides a comparison of the IA topics from the contents of the various products that were examined. Some topics, such as the use of modems, were eliminated from this list, as it was deemed that they were no longer major problems to be addressed in a Navy-wide IA Awareness program. The general principles associated with modem use are still preserved in the "changing system and network configuration" topic. Also, some specific topics were integrated into more general topics. For instance, the *natural hazards* topic addressed in the NAVSO 5239 series was integrated into a more general topic under *computer vulnerabilities*. The user behavior that must be encouraged with respect to natural hazards is also included with the topic concerning *backups*. While this may deemphasize some specific topics, it was deemed necessary so that current challenges to IA awareness could be addressed. The topics in Table 5 represent the pool of potential topics for the CyberCIEGE scenarios.

Topic	NAVSO	NIST SP 800-50	DOD CBT	DISA IA Brief
Information value determination	x	X	x	x
Password management	x	X	x	x
Physical security	x	X	x	
Suspicious activity	x	X	x	x
Changing system and network configurations	x	X		x
Using shared and networked resources	x			

Topic	NAVSO	NIST SP 800-50	DOD CBT	DISA IA Brief
Computer vulnerabilities	x	X	x	
Internet security (e.g. E-commerce)	x	X	x	x
Virus prevention and detection	x	X	x	x
Self-monitoring	x	X	x	
Reporting procedures	x	X	x	x
Network vulnerabilities	x		x	x
Unattended computers	x		x	x
Information disposal	x		x	x
Handling of classified and sensitive data	x		x	x
Differences between classified and unclassified networks	x			x
Backups and Storage	x	X	x	x
Unauthorized software use and licensing	x	X	x	x
Protecting software	x		x	
Policy and law			x	x
Critical Infrastructure Protection Program			x	
Threats and vulnerabilities			x	
Social engineering		X	x	
Malicious code	x	X	x	x
Internet hoaxes			x	
User role in system security	x	X	x	x
CAC procedures, PKI, and encryption		X	x	x
Warning banners and labels	x	X	x	x
Peer to Peer risks and policy				x
Wireless and handheld devices security		X		x
Implications of non-compliance		X		
Spam and email usage		X		x
Personal Use or Gain		X	x	x
Inventory and property transfer		X		
Laptop security on travel		X		
Personal Devices at work		X	x	x

Topic	NAVSO	NIST SP 800-50	DOD CBT	DISA IA Brief
Access control issues and least privilege	x	X		
Identity theft			x	
Ethical use			x	
IA overview and definitions		X	x	x
Importance of IA			x	
History of IA			x	
Threats to IA			x	
Incidence response	x	X	x	
System patching and configuration management		X		

Table 5. Comparison of IA Awareness and Training Products

B. REQUIREMENTS FROM INFORMATION ASSURANCE POLICY AND FEDERAL LAW

There are several policy documents that address training and awareness requirements within the context of the Navy and higher-level organizations. The documents include:

- **The Computer Security Act of 1987.** This law mandates that the objectives of periodic awareness training should focus on enhancing awareness of threats and vulnerabilities and to "encourage the use of improved computer security practices." This law also mandates that awareness training should be in accordance with NIST guidelines [CSA 1987].
- **The Federal Information Security Management Act of 2002.** This law mandates that IA awareness and training initiatives should focus on risks and responsibilities in the context of risk reduction policies and procedures [FISMA 2002].
- **DOD Directive 8750.1.** This directive states that all users of DOD information systems must receive an initial IA awareness orientation followed by annual refreshers.

- **Secretary of the Navy Instruction 5239.3A.** This instruction, entitled "The Department of the Navy Information Assurance (IA) Policy," states that annual refresher awareness training should focus on Internet Security, best security practices, risks associated with user activities, and user responsibilities to comply with risk-reduction policies and procedures [Navy2 2004].

C. ORGANIZATIONAL "FIT" AND THE APPLICABILITY OF CYBERCIEGE

There are two major organizational issues that will influence the effectiveness of Navy-wide awareness initiatives. First, a precise understanding of the organizational characteristics is hard to determine because the Department of the Navy consists of various smaller organizations with peculiar characteristics. Some organizations are based ashore, some afloat, and some are hybrids of the two. Some organizations are based overseas and some are integrated with other agencies. Second, the target audience for a Navy-wide IA awareness and training program varies with location. Some organizations are manned strictly with military members while some are integrated with civilian employees and contractors. Each category of user may view the information to be protected from a different perspective. For instance, a temporary contractor with little security training may not realize that the dissemination of some types of unclassified government information may reveal details of an operational nature. This information may be viewed as harmless by the contractor, but when viewed from a military perspective, may reveal a weakness in operational capability or reveal information about military operations. Likewise, a military member may not recognize the importance of protecting contractor information and proprietary information since this type of information is not part of most military policy statements.

A major trend in the DOD is the increase in the outsourcing of many functions that have traditionally been completed by military members. For instance, the Navy-Marine Corps Intranet (NMCI) outsourcing contract was awarded in 2000 and effectively placed the burden of network administration for

all shore-based Navy IT infrastructures in the United States on a civilian contractor. The result of the NMCI contract is that NMCI contractors are interacting with a majority of the naval organizations located in the United States. The NMCI initiative sought to standardize the administration of many of the computer networks across the Department of the Navy. Despite this initiative, the Navy was unable to completely eliminate network administration jobs. The Navy still retains network administration responsibilities for afloat locations and some overseas locations.

CyberCIEGE offers many options for addressing these organizational concerns. First, CyberCIEGE scenarios can be tailored to a particular organization with a specific set of requirements. This flexibility allows the facilitators of IA programs to create a scenario based upon whatever organizational boundaries they choose. The CyberCIEGE campaign for this thesis will focus mainly on the organizations that are primarily staffed by military personnel within the Navy. Second, a range of scenarios can be created to appeal to different user groups. A compelling scenario can be created for user groups that are attracted to the educational benefits of video games or a simple scenario can be created to communicate simple messages. The CyberCIEGE campaign produced in this thesis will attempt to address a wide range of user groups. Third, CyberCIEGE leaves a small "footprint" for installation and game play. CyberCIEGE can be installed on a network server and played across the network at various workstations. The ability to play CyberCIEGE across a network has many benefits including centralization of game logs and allowing users to complete scenarios during their free time to minimize workspace disruption.

D. PEDAGOGY

Older and Chin advocate the use of an outcome-based approach when developing Information Assurance courses [Older 2003]. The outcome-based approach offers the advantage of prioritizing educational goals according to the practical outcomes needed in the organization. This pedagogical approach is

ideal in awareness programs where the outcomes may include behavior change and varying levels of increased knowledge.

Educational outcomes were written for the topical requirements derived from this chapter. The outcomes will be taught within the contents of a CyberCIEGE campaign meant to engage the user in an entertaining fashion. The educational outcomes produced from this chapter will be discussed in the next two chapters. Specific methods that can provide feedback on the efficacy of this CyberCIEGE awareness campaign will be discussed in Chapter Five.

E. NAVY CYBERCIEGE INFORMATION ASSURANCE TRAINING AND AWARENESS SCENARIOS

Training and awareness topical requirements were developed from the Navy's legacy Information Security (INFOSEC) program and from the current DOD IA Training and Awareness Computer-Based Training course. Topics were then compared with existing NIST guidelines and the IA awareness training brief available from the DISA website. Two scenarios based on the user role relative to Information Technology (IT) were developed to fulfill the requirements for Navy IA awareness and training. The idea of separate training for different user levels is consistent with recommendations from the legacy Navy INFOSEC program. This notion is valid since the Navy still maintains network and system administrators in afloat and overseas locations.

Topical content for the scenarios originated from Table 5. Topics chosen were based on several criteria to include, current applicability to IA, relevance to the Navy, relevance to the user, and the potential to represent the topic in CyberCIEGE. Some topics such as Internet Security and Identity Theft were not covered since a scenario covering these topics already exists [Ruppar 2005]. Other topics such as wireless security were rejected since the current version of CyberCIEGE cannot support wireless devices.

The first scenario is a basic CyberCIEGE scenario that targets all users of Navy information systems and seeks to make the player aware of basic IA

problems and principles. Since the goal of this scenario is to make all users of information systems aware of IA problems, it generally falls in the “Security Basics and Literacy” category on the NIST IT Security Learning Continuum [NIST1 1998]. This is depicted with the lower arrow on Figure 4. The purpose of this scenario is to communicate information and reinforce basic practices that will increase the level of security within an organization. This scenario is primarily motivated by DOD Directive 8750.1. Educational outcomes for this scenario will be covered in Chapter III.

The second scenario is a technical scenario that targets users whose job functions are directly concerned with IT, as suggested in Figure 4. Examples of technical users in the Navy include ISSM’s, ISSO’s, system administrators, and network administrators. The focus of this scenario is on skill application and problem solving. The scenario seeks to introduce the technical user of an information system to the types of actions that will directly influence the security posture of the organization. This scenario will allow the player to modify many more items within the context of the scenario in order to discover IA principles. This scenario will also be of value to the IT Security Specialist and Professional since it will allow the player to gain understanding of IA principles in the framework of the scenario. Educational outcomes for this scenario will be covered in Chapter IV.

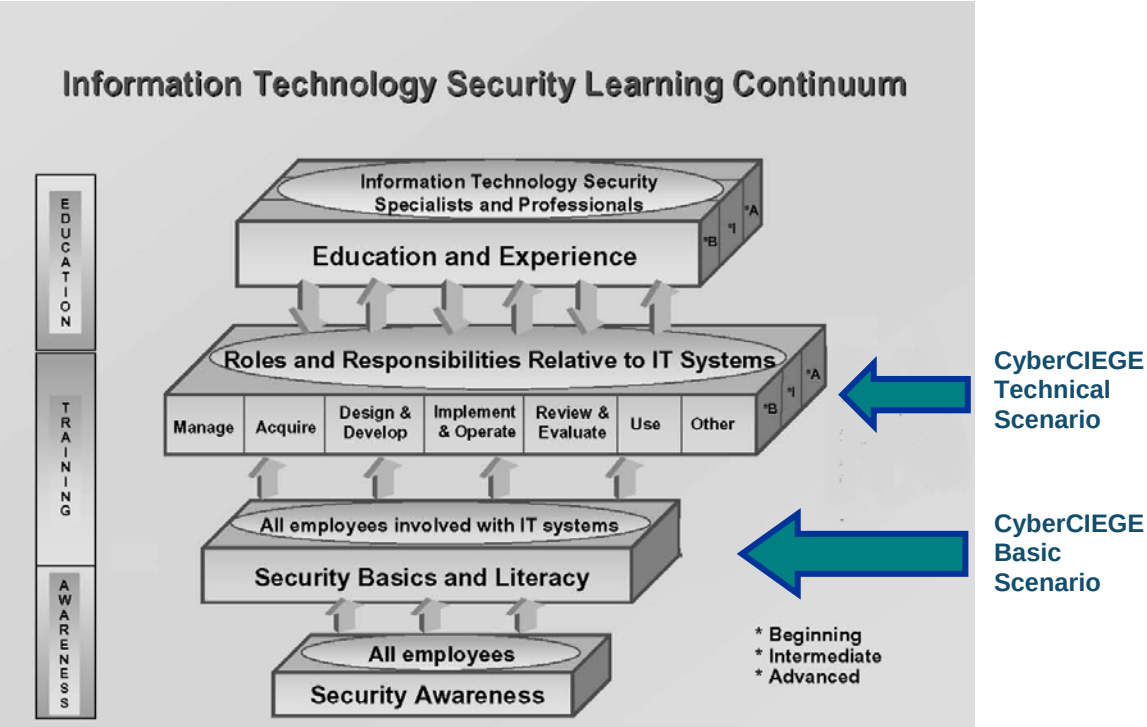

Figure 4. NIST IT Security Learning Continuum (After [NIST1 1998])

F. SUMMARY

This chapter covered the requirements discovery process for this thesis. The next two chapters are a detailed description of the scenarios conceived in this chapter. The next two chapters will include a detailed description of the topics chosen from this chapter. In addition, they will describe how these topics were addressed within the context of the CyberCEIGE scenarios.

III. BASIC USER SCENARIO OUTLINE

This chapter provides a description of the basic user scenario developed to provide general user awareness. This chapter includes a description of the intended users, a description of the educational outcomes of this scenario, a description of the specific elements used to construct the scenario, and a list of the IA awareness topics that this scenario addresses.

A. SCENARIO OVERVIEW

The basic user scenario focuses on basic principles of Information Assurance and is intended for all information system users. In this scenario, the game player is placed in charge of making security decisions within the context of a small military organization. The game player must complete objectives in order to protect the security of the organization. If a game player does not complete the objectives within a predetermined period, appropriate attacks are triggered by the game engine and the game player will lose money as a result of successful attacks. After the user completes each objective, an awareness message is presented that relates the action taken in the game with real-life circumstances and provides feedback regarding the player's choices. The player will win the game if he completes all the objectives of the game without spending or losing all of the money that he was allocated.

B. INTENDED USERS

The intended audience of this scenario consists of all information system users within the context of the Navy. This is a large user group and consists of those with various job responsibilities that require the use of Information Technology. Some users of this scenario may only use computer systems for occasional training sessions and email, while others may have job responsibilities that predominantly use technologically-sophisticated information systems. Due to the varied responsibilities of the user community, a broad

approach had to be taken with respect to topics. This approach had to be mechanical at times due to the number of topics covered and the broad range of intended users.

C. USER EDUCATIONAL OUTCOMES

User educational outcomes were developed using a modified Bloom's Taxonomy as advocated by Older [Older 2003]. Individual descriptions of each of the educational outcomes for this scenario are listed below.

1. List the Attributes of Information Assurance

The purpose of this outcome is to ensure comprehension of the components of IA. Basic understanding of the attributes will challenge the game player into thinking about how to achieve IA. The user is presented with a definition of IA and a list of IA attributes in the initial briefing. The game player may choose to read the full briefing for the scenario where he will find amplifying information concerning the attributes of IA. All definitions are consistent with terminology from U.S. military doctrine as defined in Joint Publication 3-13 titled "Joint Doctrine for Information Operations [Joint 1998]."

2. Evaluate the Relative Value of Information

The purpose of this outcome is to ensure that the game player can analyze information assets and determine whether additional safeguards are necessary. The first objective that the game player must complete is to ensure that the Personnel Database is protected with an Access Control List (ACL). The player must locate the personnel database and ensure that the "Protect with ACL" component setting is set. Once the player completes this objective, he is required to take a short quiz in which he is asked about whether he thinks that the personnel database needs to be available to all personnel. Appropriate feedback is given to the game player to ensure that he knows that, although unclassified, personnel information needs to be protected from unnecessary

disclosure. The second question of the quiz requires the player to make a decision about whether pictures from a command picnic should be available to all personnel. Once the player answers the question, appropriate feedback is given to reinforce the idea that this type of information should be available to all personnel.

3. Recognize Common Activities That Lead to Malicious Software

The purpose of this outcome is to ensure that the player can describe activities that are potentially harmful and may weaken anti-virus defenses. The player is given an objective in which he must look through a list of component settings for a computer and select three settings that will help prevent the installation of malicious software on a computer.

4. Describe the Consequences of Not Locking Unattended Computers

This outcome seeks to ensure that the user understands one of the most basic vulnerabilities caused by all levels of users. The player is given an objective in which he must set policy ensuring users lock or logout from a particular computer. The player is informed that he must do this in order to ensure that unauthorized users do not have access to the system. The policy that the user must select is part of a list of procedural settings that the user can select for any component within the game.

5. Describe the Consequences of Poor Password Protection

This outcome also seeks to ensure that the player understands one of the most common vulnerabilities in an information system. The player is given an awareness message that communicates that passwords should never be shared. After this message, the player is presented with an objective that seeks to prevent the accidental disclosure of a password to an unescorted contractor. In this objective, the player must, in a timely manner, set a policy which states that users are not allowed to write down passwords.

6. Recognize Basic Physical Security Mechanisms

This outcome seeks to ensure that the player is familiar with various physical security mechanisms. Raising the awareness of physical security mechanisms will help the player recognize when things are "not right" within his own workplace. In the scenario, the player is presented with an objective that states the user must raise the level of security to a predetermined level. The player must decide which mechanisms are the most cost-effective.

7. When Given a Scenario, Be Able to Identify and Report Suspicious Activity

The user is presented with different circumstances that may or may not lead to a social engineering attack. The social engineering scenario is loosely based upon various social engineering and influence tactics described by Kevin Mitnick [Mitnick 2002]. In the scenario, the player is asked a question which states:

> Bob Woodstein called to interview you for some background for his next newspaper story. He said that he talked to Captain Ahab about it after he read about your command picnic in the base newspaper. Will you give him enough time out of your busy schedule to answer a few questions so that your command can finally get some good publicity?

The question has several subtleties that may influence the player's answer. First, Bob Woodstein calls and wants to "interview" the game player. The game player is being asked to assist someone he thinks is a reporter. Within the scenario, the player is put in the spotlight as someone important enough to be interviewed for a newspaper story. Second, the caller claims that he talked with the player's Captain, who is presumably someone in authority. This is a subtle appeal to the player that some sort of "authority" has authorized this interview. Third, the game player is put in the position of "enabling" good publicity about the organization. The word "finally" is inserted into the question to force the game player to think that the organization has had bad publicity lately and that this is a chance for the game player to do something positive for the organization.

After the player answers this question, he is presented with the social engineering objective in the game. This objective contains a definition of social engineering and describes how this type of attack may occur, specifically that an attacker typically needs a combination of time, work, indifference to detection, special access, and knowledge to complete an attack [Murray 2005]. The objective then instructs the player on how to prevent a "social engineering" attack from occurring. Of course, depending on how the player answered the first question, he may already be at a disadvantage within the scenario.

The game player is then told that the game character "Ensign Pulver" lost his ID and needs it replaced. If the game player does not choose to replace the ID, then the player is informed that he must escort Ensign Pulver on base and a penalty is assessed. At a predetermined time in the scenario, the player is given feedback on the social engineering objective. This feedback message informs the player that the person claiming to be Bob Woodstein had stolen Ensign Pulver's ID. The player is also given procedures that should be followed when observing suspicious activity. If the player chose to be interviewed by Bob Woodstein, the social engineering feedback message would be reinforced because an attack would have been triggered in the game engine.

D. SCENARIO ELEMENTS

1. Briefing Screens

The initial briefing is the first screen of the game that the game player sees. In this scenario, the initial briefing serves to provide the context for the scenario and provides basic information for the scenario. The initial Briefing screen is illustrated in Figure 5 and states the following:

> You have been put in charge of Information Assurance for your command. Your goal is simple: Protect your organization's computer systems by completing the objectives of the scenario. You must do this while saving the most money possible.

You will explore situations that will examine Information Assurance principles. Click on the GAME tab for a full description of the attributes of Information Assurance. You can type 'e' at any time to bring up the CyberCIEGE encyclopedia. There you can learn how to play the game, and read or watch movies about various Information Assurance topics.

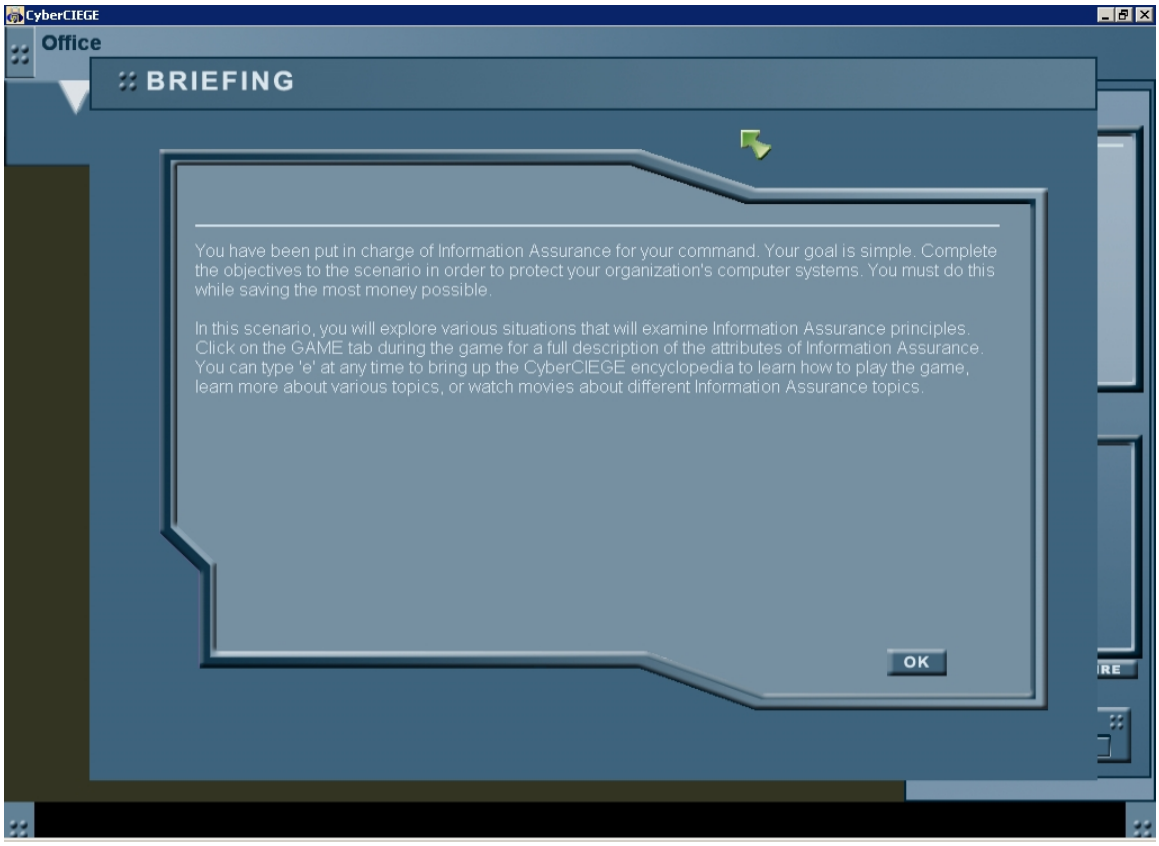

Figure 5. Basic Scenario Briefing Screen

The initial briefing screen references the full brief located in the Game tab. In this scenario, the full brief serves one main purpose. It provides definitions of IA and the attributes of IA. This reinforces the first educational outcome of being able to list the attributes of IA. The two IA products that were analyzed in Chapter II included definitions of IA and IA attributes. Specifically, the full briefing states that:

Joint Pub 3-13 defines Information Assurance as Information Operations that protect and defend information systems by ensuring their AVAILABILITY, INTEGRITY, AUTHENTICATION, CONFIDENTIALITY, AND NONREPUDIATION. It goes further to say that this includes the restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance is comprised of five attributes. Often, when you do something that affects one attribute, it may have an effect on the others. The goal of this training is to help you understand some of the basic mechanisms of Information Assurance, how they interact, and why it is important for everyone to be familiar with and supportive of your organization's security posture. The attributes of Information Assurance are:

- Confidentiality: Protection from unauthorized disclosure
- Integrity: Protection from unauthorized change
- Availability: Assured access by authorized users
- Authentication: Verification of originator
- Non-repudiation: Undeniable proof of participation

2. Game Characters

CyberCIEGE has two general types of game characters. The first type of character is a user. The user is typically assigned an asset goal that must be accomplished in the course of a scenario. As discussed in Chapter I, a user can be assigned to predetermined departments, mandatory secrecy and integrity levels, and to discretionary access control (DAC) groups. User trustworthiness, training, and happiness are all variables tracked within the game engine and factor into various attacks that are conducted against the organization. The second type of game characters are support staff. Support staff characters serve in security and technician roles in the scenario. Like users, they are predefined in the Scenario Definition File (SDF). Unlike users, support staff can be hired and fired. Support staff characters have predefined hardware skills, software skills, and social skills that will determine how effective they are in the game. Support staff characters are not used to conduct attacks in the game. Table 6

summarizes the attributes for each character as initially set in the SDF. All numerical attributes are on a scale of 1-100. All attributes are on a linear scale with the exception of trustworthiness. Trustworthiness is used in conjunction with background checks to determine whether a character can be bribed. The following sections describe the different game characters in this scenario.

Character	Department	Clearance	Trustworthiness	Initial training	Happiness
Bob	Contractor	Unclassified	10	55	55
Ensign Pulver	Supply	Secret	75	5	99
Chief Goat	Operations	Secret	78	34	3
Ensign Webster	Support Staff Technician	Undefined	N/A	N/A	N/A
LT Roberts	Support Staff Security	Undefined	N/A	N/A	N/A
Petty Officer Price	Operations	Secret	90	100	70
LT Smith	Admin	Top Secret	90	55	75
Seaman Jones	Admin	Secret	72	23	89

Table 6. Game Character Attribute Summary

a. Bob the Contractor

This character is a contractor from the shipyard who is working in a space that contains a server. This character does not have an assigned computer. This character is working in a sensitive location, but is only cleared to see unclassified information. Key attributes of this character are low trustworthiness, mid-level happiness, and mid-level training.

b. Ensign Pulver

Ensign Pulver is based upon a movie character. His official job is the Laundry and Morale Officer. This character has a secret clearance and belongs to the Supply department. Key game characteristics of this character are high trustworthiness, high happiness, and low training.

c. Chief Goat

Chief Goat works in the Operations department, and has access to the Operations department DAC group. He is modeled after a senior enlisted member of the Navy. He is the assigned user to the file server. Key game characteristics include high trustworthiness, low happiness, and low training.

d. Ensign Webster

Ensign Webster is part of the support staff and can be hired as IT support in this scenario. His official title is ADP officer. Ensign Webster has low social skills, high hardware, and high software skills.

e. LT Roberts

LT Roberts is part of the support staff and can be hired as a security officer. In the scenario, he takes the role of the Duty Officer and is responsible for enforcing the organization's physical security policy. LT Roberts has high social skills, low hardware, and low software skills.

f. Petty Officer Price

Petty Officer Price is a modeled after a mid-level enlisted member of the organization. He has a secret clearance and is assigned to the Operations department. All game characteristics are high and he is assigned to a workstation computer.

g. LT Smith

LT Smith is the Administrative Officer. She has a top secret clearance and is assigned to the Admin department DAC group. Unlike the other game characters, LT Smith has a high security clearance. This ensures that a higher background check was conducted on her. Key characteristics include high trustworthiness, high happiness, and mid-level training.

h. Seaman Jones

Seaman Jones is modeled after a lower-level enlisted member. He is assigned to the Admin department DAC group and has a secret clearance. Key characteristics include high happiness, high trustworthiness, and low training.

3. Assets

Assets are things that are valuable to an organization. In CyberCIEGE, game assets are accessed by virtual characters through the use of asset goals. Information can be an asset. An asset's confidentiality and integrity must be appropriately protected while simultaneously being made available to those who need access. The following sections describe the assets that are defined in the basic user scenario.

a. Personnel Database

This is the organization's database that contains personal information, including counseling and evaluation reports on all personnel. It has an unclassified secrecy label. The intended access for this asset only includes the Administrative department.

b. Muster Reports

These are the muster reports for the organization. They contain the location of all personnel assigned to the organization. This asset has an unclassified secrecy label. The intended access for this asset is the Operations and Admin departments.

c. Command Picnic Pictures

This asset consists of pictures taken at an organization-sponsored picnic and are meant to enhance morale. This asset has an unclassified secrecy label. Intended access is for the Public DAC group.

d. Operations Plans

This asset contains planning documents for the Operations department. It has an unclassified secrecy label. The intended access for this asset is the Operations department DAC group. This asset has a high value and is used as a target for attackers in the scenario.

4. Secrecy

Secrecy labels tags are predefined in scenario definition files (SDF). In this scenario, three secrecy labels were defined to match government classified information. The three secrecy labels used in this scenario from lowest secrecy to highest are unclassified, secret, and top secret. While all of the assets in the SDF are unclassified, several users have different clearances which correspond to different background checks for those characters. For the purposes of this scenario, no classification for confidential material was used.

5. DAC Groups

DAC groups are defined in the SDF. This scenario uses three DAC groups that serve as department-level groups for a generic organization. The first DAC group is the Admin department which is intended for members of the Admin department. The second DAC group is the Operations department which is intended for members of the Operations department. The third DAC group is the Public DAC group which is predefined in the CyberCIEGE game.

6. Networks and Components

This scenario takes place in a small office aboard a ship. There is one local area network (LAN) to which three workstations and a server are connected. An Internet router connects the LAN to the Internet. Figure 6 illustrates the office screen for this scenario.

Figure 6. Basic Scenario Office Screen

7. Objectives

This scenario utilizes objectives to allow the player to progress through the game. Descriptions of individual game objectives are listed below.

a. Personnel Database Access Control List (ACL)

This objective requires the player to set a component setting to protect an asset with an ACL. This objective seeks to make the player aware that there are DAC mechanisms that can complement MAC mechanisms such as data classification. The player must locate the computer that contains this asset and then set the proper setting for the computer. If the player does not complete this objective in a predetermined amount of time, an attack on the database is triggered. Specifically, this objective states:

> Your first task will be to apply an Access Control List (ACL) to the Personnel Database in the Admin dept. The Personnel Database is an asset that must be used only by the Admin dept. Set the "protect with ACL" procedural setting to protect this asset with an ACL via the component tab. You should do this quickly as there might be someone who wishes to access and then disclose this information. You can find out where the Personnel Database is located via the "Asset Tab." If you would like to look at the ACL after you have selected the proper setting, click on "ACL" on the asset list (bottom right of component screen) to look at the current file permissions.

While completing this objective, the player is introduced to some of the information available from various CyberCIEGE screens.

b. Unattended Computers

The player is given a description of a vulnerability to a computer under his control. Additionally, there has been an incident that involved non-repudiation and authentication which implicitly communicates that there is a potential threat. The user is then asked to change a procedural setting on this computer. Specifically, this objective states the following:

> Security has become lax on the file server. File server users regularly leave the office with their accounts logged on and wide open. Many people have noticed, but have not said anything. Captain Ahab recently got an email from Chief Goat that Chief Goat denied sending. Help the users of the file server and change the procedural setting on the computer to force them to lock or logoff when they leave it unattended.

This objective addresses a topic that is pertinent to all organizations at all levels: the risks associated with leaving a logged on computer unattended.

c. Malicious Software Prevention

This objective deals with changing some procedures on a computer in order to help prevent malicious software. This objective requires the player to select the proper computer and determine from a list which procedures will help prevent malicious software. This objective states the following:

> LT Smith is new to the command. Her computer needs three procedural changes to get it up to the same level of protection

> against malicious software that other computers in the command have. Select the component tab, click on "LT Smith's Desktop," and choose the proper procedural settings.(Hint- You should regularly do something, What can be attached to an email?, and has the software been approved to operate on your system?) If you still need more help, go to the encyclopedia (use the "e" key). You will find useful information on malicious software as well as an instructional video.

A hint is explicitly given in the objective in case the player has trouble determining which settings are appropriate. The player is given a predetermined amount of time to complete the objective. If he does not complete the objective in time, an attack is triggered in the game which targets an asset with malicious software.

d. Password Management

This objective seeks to teach the player about proper protection of passwords. The player must prohibit users from writing down their passwords. Specifically, this objective asks the player to do the following:

> Chief Goat left his password written down on a post-it note on the file server. Unbelievably, this procedure is currently allowed on the file server! Click on the component tab, find the file server, and uncheck the ”allow writing passwords” procedural setting to correct this. You must do this before an untrustworthy person uses this password to maliciously use the system.

An appropriate attack is triggered after a predetermined amount of time if this objective is not completed. This objective is also utilized in conjunction with popup messages to communicate to the user some of the hazards of sharing passwords and to support one of the educational outcomes.

e. Social Engineering

This objective seeks to inform the user about Social Engineering and how an attack may occur. This objective states the following:

> Social Engineering is a term used by security professionals that describes a technique by which an attacker uses deception or

> persuasion to gain access to an information system. Typically, a social engineer needs a combination of time, special knowledge, and access to successfully infiltrate an information system. Your objective is to prevent a successful social engineering attack from occurring during this scenario.

This objective is meant to alert the user to be ready to prevent an attack. It is intentionally vague in order to alert the player to remain vigilant. The specifics of this part of the scenario were described in a previous section. Depending on how the player responds to the scenario, an attack is triggered in which an intruder breaks in and steals random computer media as determined by the CyberCIEGE game engine. This objective is complete at a predetermined time in the scenario when appropriate feedback is communicated in a pop-up message.

f. Data Protection and Backups

This objective seeks to make the player concerned about game characters taking government information media containing personnel information out of the office. The player is asked to discover and select a procedural setting to ensure that government information media stay at work. In the course of completing this objective concerning taking government information out of the office, the player is also instructed about the importance of backing up data offsite. This objective states the following:

> LT Roberts reported to you that he saw LT Smith going home with a CD labeled "Personnel Database." Click on component and determine which procedural setting to set on LT Smith's desktop that you will use to tell LT Smith to keep government computer media at work and to not take it out of the proper zone.

This objective leads the player into selecting a procedural setting that prevents users from taking media from the office. Once the objective is completed, the player is given a pop-up message that explains the circumstances in the scenario and that the game character was protecting the data by storing a back-up copy in a vault off-site before she went home. The player is informed that the report was a false alarm and instructed that it is essential to store backups off-site.

g. Physical Security

This objective allows the player to choose a set of cost-effective physical security mechanisms to raise the physical security of the office to a specific level measured by the game and displayed to the player in the Zone tab. Specifically, the objective states the following:

> After several questionable incidents that were reported to the Captain through the Security Manager, Captain Ahab has given you $5000 to increase the level of physical security throughout the entire office to 300. Click on the "zone" tab and peruse the physical security options on the lower left hand portion of the screen. Buy various mechanisms to improve the physical security level throughout the entire office. Be careful not to go broke, otherwise you will lose the game and have to start over.

This objective directly supports the physical security outcome. The player must evaluate different security mechanisms within the constraints of his budget. If the player runs out of money, he loses the game.

E. KEY SCENARIO TOPICS

This section describes how the topics chosen and developed in this scenario correspond to the topical requirements enumerated in Chapter II. In general, some topics such as personal use of email were avoided since guidance concerning email policy is often promulgated at low levels and varies with organizational mission, size, communication bandwidth, operational tempo, and personnel. The following list summarizes the topics covered and describes how this scenario presents them to the user. These topics include:

- A definition of IA and IA attributes. The player is explicitly given definitions for IA in the full briefing. The player is also exposed to the application of these definitions by completing the game objectives.
- Information value determination. This topic communicates to the player that some information assets may be more valuable to the organization than other assets. The player must complete a quiz

with appropriate feedback that specifically asks him whether some assets require more protection than others.

- Access Control. This topic introduces the player to the concept of access control and that there are mechanisms available to protect information. The player must protect an asset with an Asset Control List (ACL).
- Social engineering and suspicious activity. This topic teaches the player to discern whether or not it is appropriate to release information to an unknown person. The player is asked whether he would take part in an interview about his organization. The player is then introduced to the idea that an attacker can use seemingly harmless information together with various mechanisms to attack the organization.
- Password protection. The game player is introduced to appropriate password protection practices. The player must complete an objective which prohibits virtual users from writing down their passwords. After completion of this objective, the user is presented with a pop-up message explaining the dangers of sharing passwords.
- Malicious software and basic safe computing. The player must discover different practices to protect a computer from malicious software. Specifically, the player must select different procedural settings for a computer that will limit malicious software propagation.
- Backups and data storage. The player is introduced to the idea of off-site backup through the use of a pop-up message within the scenario.
- Physical security. The player is introduced to different physical security mechanisms that will increase physical security.

Specifically, the player must purchase cost-effective mechanisms to increase security in the organization.

- User role in system security. The game player is introduced to reporting procedures and his role in security. Self-monitoring and vigilance are advocated as an extra layer of security. This topic is explicitly addressed in the feedback provided from the social engineering objective.
- Unattended computers. The player is presented with a scenario in which a contractor is left alone in a room with a computer that a user has logged into and left unattended and unlocked. The player must set policy that forces a virtual user to lock or logoff from this computer when he leaves it unattended.

F. SUMMARY

This chapter has described the basic user scenario created as a part of this thesis. The next chapter describes the technical user scenario.

IV. TECHNICAL USER SCENARIO OUTLINE

This chapter provides a description of the technical user scenario intended for users who are directly involved in some aspect of information systems management and allows the player a larger degree of autonomy in completing the scenario than the basic user scenario presented in Chapter III. This chapter provides a description of the intended users, a description of the educational outcomes, a description of the CyberCIEGE elements used in the scenario, and a list of IA topics that the scenario addresses.

A. SCENARIO OVERVIEW

This scenario focuses on network security and it serves to introduce technical users to the roles that they will perform that influence security. The game player takes the role of security manager while the "boss" is away. In this role, the game player must manage three internal networks, one of which processes classified information. To complete the scenario, the player must let the game engine run for 10 "game" days until the player's boss returns to take over the security management role. During this time, the underlying game engine executes triggered attacks against the networks and the player is given a chance to respond, adjusting his network security settings in order to increase their protection. Successful attacks against the player's system will cost the player money as will changing the system configuration. The player will win the scenario if he has money left over at the end of the game. This scenario differs from the basic scenario in that it focuses on observation and remediation. The player must observe which attacks are successful and prevent them from reoccurring. While this scenario does have educational outcomes, it also allows the player to learn practical applications of security principles by adapting and creating his own solutions to attacks.

B. INTENDED USERS

The intended user group for this scenario consists of all Navy personnel with roles and responsibilities related to the management of information systems. This scenario assumes that the game player will have basic knowledge of security concepts and a mastery of those presented in the basic scenario.

C. TECHNICAL USER EDUCATIONAL OUTCOMES

Educational outcomes for this scenario consist of a set of abilities related to computer network defense. For each of the items listed below, the player should be able to execute the predicate.

1. Identify the Uses of Access Control

This outcome seeks to ensure that the player is aware of different access control mechanisms and their uses. The user must complete an objective that forces the player to change an ACL. The player is also exposed to other access control mechanisms throughout the scenario including password policy, physical access, least privilege, DAC groups, and information classification levels.

2. Identify the Need for Regular Backups of Important Data

The user must complete an objective that sets policy for off-site backups in order to ensure availability.

3. Describe Various Criteria for Passwords and Determine Their Effect on Password Management

This outcome seeks to expose the player to different considerations for setting password policies. Specifically, the player must complete an objective that sets password policy for two computers that contain shared resources.

4. Describe the Function of Anti-virus Tools

This outcome seeks to expose the player to considerations for anti-virus tools. The player is forced to decide between automatic and regular anti-virus updates.

5. When Given a Physical Layout, Identify Physical Control Mechanisms That Will Enhance the Overall Security

This outcome is used in conjunction with two objectives that force the player to analyze the physical layout of the organization and decide where best to apply cost-effective physical security controls. The player is also forced to discover which areas need a higher level of physical security.

6. Describe the Security Features of Various Network Devices

The purpose of this outcome is to ensure that the player has an understanding of the basic function of network devices and their role in security. Specifically, the player should learn that filtering can be executed at routers and that routers separate networks. The network architecture supports this outcome as well as several objectives, including the filtering objective, the network vulnerability testing objective, and the operational network objective. While accomplishing these last two objectives, the player has the opportunity to buy network components to enhance security if he deems it to be cost-effective.

7. Describe Basic Computer and Network Security Mechanisms

This outcome seeks to ensure that the user understands various mechanisms to support system security. This outcome is supported by multiple objectives and by the ability of the player to modify the security mechanisms of the scenario in response to various attacks. This outcome is limited by the choices allowed by the CyberCIEGE game itself.

8. Describe the Issues Associated With Updating Software

This outcome seeks to make the player aware of basic issues surrounding software updates. The player is presented with information describing the advantages and disadvantages of software update configurations. The player must then choose which update configuration he wants to use.

9. When Given a Scenario, Determine Appropriate Controls for an Observed Attack

This outcome seeks to take the attacks triggered within the CyberCIEGE game engine and force the player to respond to these attacks within the constraints imposed by the scenario. The player must make decisions to determine how best to prevent a reoccurrence of an attack.

D. SCENARIO ELEMENTS

This section describes various elements of the technical user scenario.

1. Briefing

The initial briefing screen provides the context for this scenario. The initial briefing states the following:

> Your boss, the Command Security Coordinator had to go out of town for 10 days. He left you with the task of managing the security of the computer networks and achieving the IT objectives for the Command. His biggest concern was that both servers needed some attention and that the Admin department desperately needs two computers. He left you in charge of three internal networks, one of which handles classified information (siprlan) and is connected to the SIPRNET. He left you a list of things to do in the form of objectives. Your task will be to secure the network while staying within budget and achieving your objectives. You will have a chance to test your security measures for one hour of game time to fine tune your settings in the middle of the scenario. During the last portion of the scenario, you will have to let your network go operational for at least 10 days of game time until your boss gets back. Good luck and don't go broke!

The full briefing consists of the initial briefing and a list of the educational outcomes as described in Section C.

2. Game Characters

This section describes the characters in this scenario. Virtual users are assigned to secrecy groups, DAC groups, and asset goals which will be described in subsequent sections. Table 7 summarizes the initial attributes of the virtual users. Support staff characters are described in Section i. The

Support Staff characters are those game characters who the player may use during the course of the game for technical or security functions.

Game Character	Department	Clearance	Trustworthiness	Initial Training	Happiness
LTJG Woodward	Communications	Secret	95	70	90
PO3 Packard	Communications	Secret	70	70	70
PO1 Dell	Operations	Secret	40	90	70
MCPO Gates	Ship's Company	Confidential	75	90	75
PO3 Torvalds	Ship's Company	Unclassified	90	90	99
LT Dewitt	Operations	Secret	95	60	80
Chief Hewlett	Admin	Secret	80	85	90
Seaman Jones	Admin	Confidential	55	60	80

Table 7. Summary of Virtual User Attributes

a. LTJG Woodward

Lieutenant Junior Grade Woodward is the Communications and Automatic Data Processing (ADP) officer. He is assigned to the Communications division and has a secret security clearance. He belongs to the Public, Communications Division, and Ship's Company DAC groups. This user has two asset goals that must be completed during the course of the game. His first asset goal is to have Internet Access. His second goal is to have access to the Woodward's Stuff asset. By default, this character has access to a classified computer in the Operation's department that he does not need access to.

b. PO3 Packard

Petty Officer Third Class Packard is assigned to the Communications division. He has a secret security clearance and belongs to the Public, Communications Division, and Ship's Company DAC groups. This user is assigned the Internet Access asset goal and access to Packard's Stuff goal.

c. PO1 Dell

Petty Officer First Class Dell is assigned to the Operations department. He has a secret security clearance and belongs to the Public, Operations department, and Ship's Company DAC groups. This user has three asset goals: Internet access, access to Dell's Stuff, and access to the Readiness Reports of the organization.

d. MCPO Gates

Master Chief Petty Officer Gates is the senior enlisted member of this organization. In his capacity as the senior enlisted member on the ship, he belongs to the Ship's Company department. He has a confidential security clearance and belongs to the Public and Ship's Company DAC groups. This character has two asset goals which are Internet access and access to Gates' Stuff.

e. PO3 Torvalds

Petty Officer Third Class Torvalds is also assigned to the Ship's Company. He is only cleared to access unclassified material. He belongs to the Public and Ship's Company DAC groups. His assigned asset goals include Internet access and access to Torvald's Stuff.

f. LT Dewitt

Lieutenant Dewitt is the Operations Officer. He belongs to the Operations department and has a secret clearance. He belongs to the Public, Operations department, and Ship's Company DAC groups. LT Dewitt's asset goals include access to Dewitt's Stuff and access to the secret material stored on the Ship's SIPRNET Server.

g. Chief Hewlett

Chief Hewlett is the Administrative Officer. He is assigned to the Admin department and has a secret clearance. He belongs to the Public, Ship's

Company, and Administrative department DAC groups. Two asset goals are assigned which are Internet access and access to Hewlett's Stuff. These asset goals do not influence the scenario until the game player completes the objective that results in the purchase of two workstations for the Admin department.

h. Seaman Jones

Seaman Jones works in the Admin department and has a confidential clearance. He belongs to the Public, Ship's Company, and Administrative department DAC groups. Two asset goals are assigned to this character to include Internet Access and access to Jones' Stuff. Like Chief Hewlett, these goals do not influence the scenario until two workstations are purchased for the Admin department.

i. Support Staff

There are ten possible support staff characters that may be hired for this scenario. Three of these characters may be hired for physical security. These security characters come with different skills and costs associated with their jobs and it is up to the game player to decide what combination will be most effective in the scenario. The three possible security staff characters are named LT Roberts, Ensign Pulver, and Seaman Dowdy. There are seven characters who may be hired as IT technicians. Like the security staff, these characters come with various benefits and costs and it is up to the game player to decide which IT staff to hire. The seven technicians that may be hired by the player include PO1 Farragut, PO1 Spruance, PO2 Bulkeley, PO2 Nimitz, PO3 Halsey, Seaman Dewey, and Seaman Nelson.

3. Assets

This section describes the assets in this scenario.

a. Web Resources

This asset is located on the Internet and its sole purpose is to be used in conjunction with the Internet Access asset goal to ensure that the game player does not disconnect any game characters from the Internet.

b. Deployment Schedules

The Deployment Schedules asset is the long-term schedule for deployments within the organization. This asset is classified secret and its access is limited to the Operations department. There is a high cost associated with disclosure of this asset and there is high motive for non-Operations department personnel to have access to this asset.

c. Crew Evaluation Reports

This asset contains the evaluation reports for the entire command. This asset is unclassified, but access is limited to the Admin department. There is a high cost associated with compromising this asset as well as high motive to attack this asset.

d. Secret Manuals

This asset contains training manuals that are classified secret. This asset is located on the Ops SIPRNET workstation that is assigned to LT Dewitt. There is a high penalty and motive for disclosure of this asset.

e. Readiness Reports

This asset contains information on the current operational capabilities of the organization. This asset is classified confidential and is located on the SIPRNET Server. There is a high penalty and high motive associated with this asset.

f. Game Character's Stuff

Each individual user stores work-related information on various workstations. These assets are used in conjunction with associated asset goals to ensure that each user has access to their work-related assets. These assets are generally located on the individual workstations that are assigned to each user.

4. Asset Goals

This section describes the asset goals in this scenario.

a. Game Character Stuff Access

Each user is assigned individual asset goals that govern access to their own information. These goals are necessary in order to ensure that user access to their own work is maintained.

b. Internet Access

This goal is used in conjunction with the Web Resources asset to ensure that all users who need Internet access have Internet access.

c. Secret Material Access

This goal is used in conjunction with the Secret Manuals asset to ensure that LT Dewitt has access to the Secret Manuals.

d. Readiness Report Access

This goal is used in conjunction with the Readiness Reports asset to ensure that PO1 Dell can access the Readiness Reports.

e. Deployment Schedule Access

This goal is used in conjunction with the Deployment Schedule asset to ensure that the Operations department personnel have access to the Deployment Schedule.

f. Eval Report Access

This goal is used in conjunction with the Evaluation Reports asset to ensure that the Admin department has access to the crew Evaluation Reports.

5. Secrecy

This scenario uses three secrecy labels that correlate to U.S. military information classifications. These labels include unclassified, confidential, and secret.

6. DAC Groups

This scenario uses several DAC groups. The Public group is used for all personnel and those that may have temporary access to the system. The Ship's Company group is used for all personnel assigned to the Ship. The Operations department, Communications Division, and Administrative department groups are used for members of the various departments.

7. Physical Layout

The Physical layout for this scenario is illustrated in Figure 7. Each room contains the work area for personnel for a particular department. Individual zones and computer network topology will be described in the next two sections.

Figure 7. Technical User Scenario Office Screen

a. Zones

The scenario workspace is broken up into zones to control individual characteristics of these areas. Physical access to various zones can be restricted using the Zone Access List option in the game. The Admin zone contains the desks and workstations assigned to the Admin department. All users in the Public DAC group are permitted to enter this zone. The Operations zone contains the computers for the Operations department. This zone contains one computer connected to the SIPRNET and one computer connected to the Internet. Initially, the permitted users in this space need only belong to the Public DAC group. As with all zones in this scenario, the player can make this access policy more restrictive. The Computer Room zone contains two workstations that process unclassified information, the secret level server, the unclassified server,

and all networking equipment. By default, this zone also allows anyone from the Public DAC group access. The Entire Office zone contains all of the three previous zones as well as an overflow room that contains two more workstations. By default, the entire zone allows anyone from the Public DAC group access. The last zone is the Offsite zone. This zone is non-configurable for the player and contains the components necessary for maintaining Internet access within the game. The Entire Office zone layout is displayed in Figure 8 and includes the Operations, Computer Room, and Admin zones.

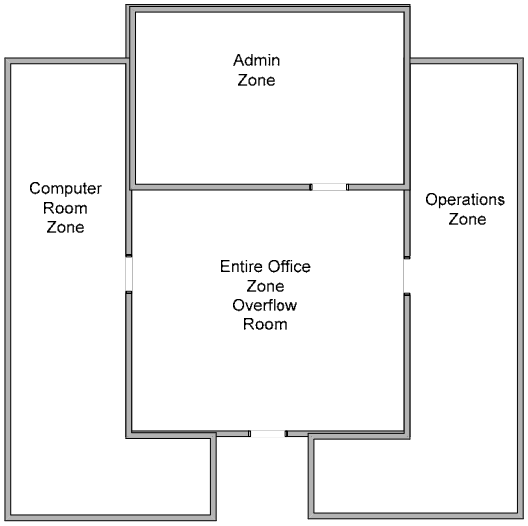

Figure 8. Zone Layout

b. Network Topology

This scenario contains three internal networks that the game player must manage. The first network is called the Siprlan network. Information classified up to secret may reside on this network. This network contains one workstation and one server. The Siprlan network is connected to the SIPRNET. The Second network is entitled the Unclass DMZ network. This network is connected to the Internet via a router and contains a server that contains unclassified information. The third network that the game player must manage is the Niprlan network. This network initially consists of five workstations. This

network will grow to seven workstations by the end of the game. This network is connected to the Unclass DMZ network via a router. The network topology for this scenario is illustrated in Figure 9.

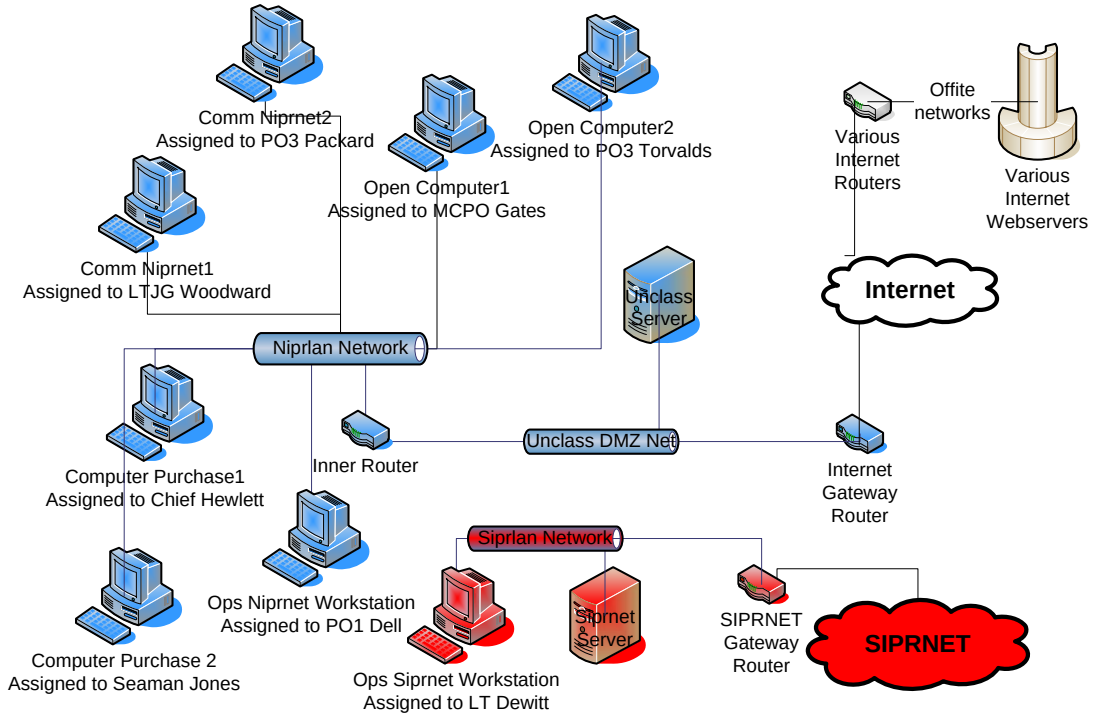

Figure 9. Technical Scenario Network Diagram

8. Phases

In addition to objectives, this scenario makes use of phases in order to teach concepts to the game player. Phase One consists of basic objectives related to network filtering, ACL's, and physical security. Phase Two seeks to make the player aware of some configurable settings that may help the player later in the game. This phase assigns objectives concerning system patches, configuration management, anti-virus mechanisms, password policies, and back-ups. In addition, Phase Two gives the player a chance to review the security settings for the various networks in preparation for phase three. Phase Three consists of a "network vulnerability test" in which the player must allow the game to run for one hour of game time. During this phase, the game player's networks

are exposed to certain attacks intended to reveal the robustness of the player's chosen security mechanisms. This phase is meant to focus the player on some weaknesses in his security. Phase Four gives the player a chance to harden his networks in preparation for Phase Five. Specifically, the player must secure the three internal networks while ensuring that all user asset goals are met. During this phase, the player must also purchase and configure two computers for the Admin department. During Phase Five, the player must allow the game to run for ten days of game time. All attacks in the CyberCIEGE game engine are triggered at different intervals during this time. This allows the player to pause the game and correct any deficiencies noted from the attacks. This phased approach supports the educational outcomes via objectives while allowing the player the latitude to explore the complexities of system security within the context of the game.

9. Objectives

This section describes the individual objectives that the player must complete while playing the technical user scenario.

a. Access Control Lists

This objective involves setting and reviewing ACL's for different assets. This objective states that:

> There are several assets on the SECRET AND UNCLASS servers that are open to all users on that system (Public group). This is a situation where Discretionary Access Control (DAC) would be appropriate. Protect these assets by using ACL's (Access Control Lists) to reflect the asset's intended access. If the wrong ACL's are set and someone not on the intended access list gains access, it may cost you later in the game. The minimum work necessary to complete this objective is to set the proper procedural setting for the two servers. This will ensure that the assets will be protected with ACL's.

b. Filtering

This objective allows the player to set up filtering rules on the routers that are connected to the Internet. This objective states that the player must:

> Set up filters on the Internet Gateway router and the niprlan2dmz router. You must ensure that users on the Niprlan network have access to shared resources on the Unclass DMZ network as well as internet access (both web and email). To complete this objective, you must prevent telnet access between the internet and the Unclass DMZ network while ensuring email and web access to the Internet. This is to comply with the security regulations for your command. If you have trouble finding the routers, use the network tab and find them on the network schematic.

c. Physical Security

There are two objectives that involve physical security. The first objective forces the player to choose physical security mechanisms to raise the security to a predetermined level. The first objective states that "your [game player's] boss has directed you to increase the level of physical security in the Entire Office zone to at least 300." The second physical security objective forces the player to analyze the physical layout of the scenario and determine which zones contain secret level information. Once the player identifies these zones, he must purchase physical security mechanisms that increase the physical security level to a value higher than the entire office zone. The second physical security objective states the following:

> You have two zones with SIPRNET access. Identify these two zones and increase the level of physical security in the areas with SIPRNET access to 400. The more you spend, the more security you will have, although at high cost. Hint: You need to hire IT staff (security) for the "guards present" or "roaming" options to increase your security.

d. Password Policy

This objective forces the player to determine which password policies he wants for his organization. This objective states that the player must:

> Set password policies for the two servers. This may also be a good time to review the settings for the rest of the computers in the command. (Hint: If a password is too simple or does not need to be changed very often, it is easy for hackers to crack. If a password is too complex and needs to be changed too often, then users will be more likely to undermine this security measure.)

e. Patching and Configuration Management

This objective seeks to inform the player of different settings with respect to system patching and configuration management that the player needs to set before the last phase. This objective states the following:

> Computers need to be updated with patches from time to time. Set the patching configuration you feel most comfortable with on the two servers. There are three different configurations each with particular advantages and disadvantages. With regular updates, there is a window of opportunity for an attacker to find a hole in your system before it is patched, but you can test the patch to ensure that it will not crash your network. With “automatic” or “as released” updates, it is harder for an attacker to exploit the window of opportunity provided by an unpatched system, but you give up the ability to test compatibility with your network or computer architecture. You also give up the ability to control when your systems are patched. After you configure patching updates, set the configuration management settings you feel most comfortable with on the servers.

f. Anti-Virus

This objective seeks to make the player aware of different anti-virus procedures. This objective states that:

> The servers do not have any Anti-Virus procedures set. You need to choose between regular or automatic updates, both of which have advantages and disadvantages similar to those described for patches.

g. Backups

This objective seeks to make the player aware of the off-site backups setting in the game. It also shows the player the cost of storing data.

This objective tells the player to “store the backups from both servers off-site in order to ensure that these assets are recoverable during various contingencies.”

h. Review Configuration

This objective is a reminder to the player that he needs to review the settings of his network in order to pass a network vulnerability test. This objective tells the player to:

> Review all the security settings for your networks. You will have to go operational for at least 1 hour to pass phase 3. This will give you an indication if there are any MAJOR holes that you will need to fix before phase 5.

i. Network Vulnerability Test

This objective gives the player a chance to determine if his networks can sustain a few predetermined attacks. This objective states that:

> You must allow the game to run for 1 hour of game time to see if they are any major holes in your networks. Do not be convinced that you have an impregnable network if no attacks occur. When you go operational in phase 5, there will be those who will attack your networks with no mercy. Feel free to use the "c" option to compress the game time.

j. Computer Purchase

The player must purchase and configure two workstations. The player must then connect these computers to the existing Niprlan network. This objective asks the player to do the following:

> Buy the admin department two desktops. Assign one to Seaman Jones and the other to Chief Hewlett (hint: drop them on the two empty desks). Connect them to the Niprlan Network to get them email and Internet access. Configure them appropriately for the next phase when you go operational!

k. Review Settings

This objective gives the player a chance to review the security settings of the scenario prior to connecting to the Internet. This objective states that "you should review all the security settings for your network before phase 5. This is always a good idea before you take things operational."

l. Asset Goals Completed

This objective ensures that all of the game characters have access to the assets for which they have a "need to know." This objective states that "you must ensure that all of the asset goals are met for all users before progressing to Phase 5 (You may have to unpause the game momentarily for the game to verify completion of this objective)."

m. Operational Network

This is the last objective of the game. The player must allow the unclassified network to operate on the Internet for ten game days. During this time, all of the attacks in the game engine are triggered in order to determine how strongly the game player has fortified his networks. The classified network may also be attacked during this time if the player has insufficient physical security mechanisms in place. This objective states that "you must allow the game to run for 10 days of game time. During this time, you can pause the game at any time to adjust your settings if you get attacked."

E. KEY SCENARIO TOPICS

This section describes how the topics chosen and developed in the technical user scenario relate to the topics identified in Chapter II.

- Physical security mechanisms. The player must purchase physical security mechanisms appropriate for the organization. Also, the player must determine where classified information is processed and provide these areas with a higher level of protection.

- Access Control. The player must manage assets subject to mandatory and discretionary access controls. The player is also exposed to other access control mechanisms such as passwords and physical access control.
- Network vulnerabilities. The player must set up filters for the networks connected to the Internet. Also, the player's networks must undergo a network vulnerability assessment prior to taking the networks operational in order to protect against common attacks.
- Virus prevention. The player must determine what settings to use to protect against malicious software.
- Backups and storage. The player must configure backup preferences for shared resources.
- System patching and configuration management. The player must set system patching and configuration management procedures.
- Password management. The player must set password policies for the organization.
- Computer vulnerabilities. The player must purchase and configure two workstations to protect against common vulnerabilities.
- Changing network configurations. The player must add two additional workstations to a local area network (LAN).
- Threats and vulnerabilities. The player must respond to various attacks against system vulnerabilities that are exploited by various threats.
- Differences between a classified and unclassified network. The player must manage networks with different levels of classification.
- Classified information handling. The player must manage assets that contain classified information.

F. SUMMARY

This chapter described the technical user scenario. The next chapter will address conclusions, implementation issues, and recommendations for further study.

V. IMPLEMENTATION AND RECOMMENDATIONS

This chapter contains three sections. The first section provides an analysis of issues identified by the author that may influence scenario development and implementation. The second section identifies areas for further study for the CyberCIEGE project and scenario development. The last section summarizes the answers to the research questions posed in Chapter I.

A. ANALYSIS OF SCENARIO DEVELOPMENT AND IMPLEMENTATION FEATURES

This section describes potential issues that scenario developers and IA training implementers may face when developing and using CyberCIEGE scenarios for organizational IA awareness initiatives.

1. Topic Choice and the Level of Centralization

The level of centralization of IA awareness training will affect topic choice. Centralized approaches work best at addressing topics concerning best practices and enterprise-wide security mechanisms. Decentralized approaches have the benefit of addressing locally-relevant practices that will directly affect the security of the local organization, although at the expense of not providing an enterprise-wide training standard. For instance, there is little use in presenting IA awareness messages for Common Access Card (CAC) procedures if most of the organization has not migrated to using a CAC for authentication. However, if CAC's are used by some local organizational entities, then it is entirely appropriate to address that topic in a local context.

Since CyberCIEGE is extensible, it can work well with most levels of centralization and is limited only by the capabilities of the CyberCIEGE components. Individual topical scenarios can be developed as new information handling, processing, and storage standards emerge. IA awareness and training scenarios covering many topics can be developed on a periodic basis as organizational practices change in response to technology development and

implementation. Standardization documents such as the DOD Joint Technical Architecture (JTA) may provide a valuable resource for CyberCIEGE scenario developers and may help to identify mandated and emerging standards that may have enterprise-wide usage.

2. Organizational Culture

Video-game based IA awareness and training mechanisms seek to provide an immersive and ongoing context for communicating essential messages. Any attempt to tailor a CyberCIEGE scenario to a particular demographic may result in a negative affect in another demographic. For instance, designing game features that appeal to youth may have the negative consequence of not appealing to more mature players. Therefore, it becomes necessary to understand the culture of a particular user group and find characteristics that appeal to a large majority of the user group in order to achieve maximum educational benefit.

3. Entertainment and Learning

In CyberCIEGE IA awareness and training scenarios that must span multiple topic areas, there is a tension between the goal of covering many topics and of developing a compelling storyline. Excessive required reading that interrupts the flow of the game may also degrade the user experience. The scenario developer's goal is to keep the audience interested long enough to communicate information that is relevant. The scenario developer can accomplish this using several techniques including appealing to a player's feeling of control and by providing an interactive environment.

4. Measuring Results

IA training implementers can use the CyberCIEGE Campaign Analyzer to review game logs generated through scenario play. Implementers can determine the effectiveness of user training through log analysis and can provide appropriate feedback to players in order maximize the educational value of their

IA awareness and training programs. Log analysis can also provide validation of scenario completion as well as give insight into game player's understanding of IA principles. If game players consistently make wrong decisions with respect to specific aspects of a scenario, a training facilitator may have an indication that the topic needs reinforcement or that the game interface is leading the player to make the wrong choice.

5. Installation Issues

CyberCIEGE can by installed on a local workstation or on a network location. For organizational IA awareness and training programs, CyberCIEGE should be installed on a network location. The main advantage for organizational IA awareness and training implementers to install CyberCIEGE on a network location is that the game logs will be centralized in one location thus making it easier for training facilitators to access and analyze them.

B. RECOMMENDATIONS FOR FURTHER STUDY

This section recommends areas for further study. It is separated into two subsections. The first subsection addresses areas of further study and development for the CyberCIEGE project. The second subsection addresses potential topic areas that could be addressed in future CyberCIEGE scenarios.

1. CyberCIEGE Game Development

The following list describes topics for further analysis and development within the larger CyberCIEGE project:

- Measurement of information retention in the context of a CyberCIEGE scenario. This study would evaluate the efficacy of CyberCIEGE as a vehicle for education and knowledge retention.
- Critical evaluation of the CyberCIEGE user interface. This study could address the CyberCIEGE interface and recommend or implement improvements.

- Development of wireless network capability. This area would develop a wireless network capability within CyberCIEGE. Wireless networks are becoming ubiquitous and exhibit many security risks that should be addressed in IA curricula. With this capability, virtual game characters would have the ability to use wireless networks as well as set up their own access points.
- Development of a larger library of artwork for scenario developers. CyberCIEGE currently has a small library of artwork for scenarios. This leads to the repeated use of the same artwork among different scenarios. For example, multiple users may appear as the same person in a particular scenario. This could cause player confusion.
- Development of a larger multimedia library for scenario developers. The addition of more movies and sound clips within CyberCIEGE scenarios will seek to increase player interest in the game by reinforcing good choices, illustrating poor choices, and providing contextual development of a scenario storyline.

2. Recommended CyberCIEGE Scenarios

The following list contains recommended topics for scenario development:

- Periodic IA awareness scenario update. Organizational IA awareness initiatives should evolve to address emerging IT security issues. This recommendation seeks to address the ongoing requirements of DOD Directive 8750.1 which mandates annual IA refresher awareness.
- Peer-to-peer networking scenario. Peer-to-peer applications can undermine some network security mechanisms. This scenario would address the threats and vulnerabilities of peer-to-peer products.

- CAC use. The CAC is increasingly being used in different authentication mechanisms in the DOD. This scenario would teach personnel where and how to use a CAC safely.
- Classified information handling procedures. This scenario would teach the proper procedures for handling classified information and the consequences of mishandling this information.

C. CONCLUSION

This thesis demonstrates that CyberCIEGE can be used to satisfy the Navy requirements for user IA awareness and training. It provides an analysis of the Navy requirements for annual IA awareness and training and contributes two scenarios to the set of CyberCIEGE IA training and awareness scenarios. The basic user scenario is designed for all those who have access to Navy information systems. This scenario can be used for Navy IA awareness initiatives and satisfies the requirements of DOD Directive 8750.1. Chapter II illustrates the fulfillment of DOD Directive 8750.1 requirements. The technical user scenario is designed for technical users who manage various information systems. The technical user scenario can be used for IA training and allows the player some level of independence in seeking solutions to IA problems. Table 8 is a list of the topics discovered in Chapter II and indicates which topics were addressed in the scenarios. Recommendations for CyberCIEGE improvement and potential scenario development were also included in this chapter.

Topic	Scenario*	Topic	Scenario*	Topic	Scenario*
Information value determination	B	Differences between classified and unclassified networks	T	Implications of non-compliance	
Password management	B,T	Backups and Storage	B,T	Spam and email usage	
Physical security	B,T	Unauthorized software use and licensing		Personal Use or Gain	
Suspicious activity	B	Protecting software		Inventory and property transfer	
Changing system and network configurations	T	Policy and law		Laptop security on travel	
Using shared and networked resources		Critical Infrastructure Protection Program		Personal Devices at work	
Computer vulnerabilities	T	Threats and vulnerabilities	T	Access control issues and least privilege	B,T
Internet security (e.g. E-commerce)		Social engineering	B	Identity theft	
Virus prevention and detection	B,T	Malicious code	B,T	Ethical use	
Self-monitoring	B	Internet hoaxes		IA overview and definitions	B
Reporting procedures	B	User role in system security	B	Importance of IA	
Network vulnerabilities	T	CAC procedures, PKI, and encryption		History of IA	
Unattended computers	B	Warning banners and labels		Threats to IA	
Information disposal		Peer to Peer risks and policy		Incidence response	
Handling of classified and sensitive data	T	Wireless and handheld devices security		System patching and configuration management	T

***** "B" denotes topics in the Basic User Scenario

"T" denotes topics used in the Technical User Scenario

Table 8. Summary of Topics Covered in Both Scenarios

APPENDIX A: BASIC USER SCENARIO DEFINITION FILE

```
//FILE:iata1.CSM
//DESIGNER:nobody
SDFid: iata1.CSM 3/9/06 11 24 AM :end
Organization:
        Name: Office :end
        Title: IA Training and Awareness Basic Scenario :end
        StartMonth: 1 :end
        StartDay: 1 :end
        StartHour: 0 :end
        StartMinute: 0 :end
        StartMoney: 2500 :end
        Budget: 50 :end
        ProfitSharing: 0 :end
        MainOfficeVersion: MS3A :end
        OffsiteOfficeVersion: small_office :end
        WorkSpaceFile: workspacestartoffice.txt :end
        Internet: true :end
        InternetStatic: false :end
        EasyTraining: true :end
        EasyACLs: true :end
        AttackTickers: true :end
        TutorialAttacks: false :end
        QuitText: Quitting Already? This training scenario should have given you a
basic introduction into Information Assurance. If you would like more information
on these topics, there are many Information Assurance Websites to include the
Navy's Infosec Website and DISA's IASE website. Information Assurance training
is mandatory for All DOD personnel and should be completed annually. :end
:end //of Organization

Site:
        Name: USS Ship's Office :end
:end  //of Site

Options:
        UseScenarioCatalogItems: YES :end
        NonServerDefaultPublicAccess: NO :end
        NetworksEverywhere: YES :end
        GuardCostsAtStartup: NO :end
:end
Camera:
        ViewCenterX: 55 :end
        ViewCenterY: 41 :end
```

```
        ViewAmountZoom: 2 :end
        ViewAmountAngle: 300 :end
:end // of Camera

AttackMasks:
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
:end // of attackMask
VIEWPOINT: // start, low left
        FromX: 110.0 :end
        FromY: 40.0 :end
        FromZ: 65.0 :end
        ToX: 120.0 :end
        ToY: 0.0 :end
        ToZ: 125.0 :end
:end // Viewpoint block

Network:
        Name: LocalAreaNetwork :end
        Static: false :end
:end //of Network

Department:
        Name: Admin :end
:end //of Department

Department:
```

```
        Name: adpsupport :end
:end //of Department

Department:
        Name: contractor :end
:end //of Department

Department:
        Name: Engineering/Maintenance :end
:end //of Department

Department:
        Name: Ops :end
:end //of Department

Department:
        Name: SECURITY :end
:end //of Department

Department:
        Name: supply :end
:end //of Department

Zone:
        Name: Entire Office :end
        Description:  :end
        Site: Main Site :end
        Art: 3a.tga :end
        Static: false :end
        StaticSelectable: false :end
        RemoteAuthentication: false :end
        AcceptPKICerts: false :end
        UseOneTimePasswordToken: false :end
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
        UseClientPKICerts: false :end
        VPNClient: false :end
        ScanEmailAttachments: false :end
        StripEmailAttachments: false :end
        AutomaticLockLogout: false :end
        SelfAdminister: false :end
        SelfAdministerMAC: false :end
        UserRunsPrivileged: false :end
        BlockRemovableMedia: false :end
        EnforcePasswordPolicy: false :end
        BlockLocalStorage: false :end
```

BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
// Start Default Component Settings
HoldsUserAsset: true :end
ProtectWithACL: true :end
WriteDownPasswords: true :end
LockorLogoff: false :end
PasswordLength: short :end
PasswordCharacterSet: any :end
PasswordChangeFrequency: never :end
NoEmailAttachmentExecute: false :end
NoExternalSoftware: false :end
NoUseOfModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: false :end
ApplyPatches: false :end
LeaveMachinesOn: false :end
NoPhysicalModifications: false :end
UserBackup: false :end
// End Default Component Settings
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
ModeratePerimeterAlarms: false :end
Re-enforcedWalls: false :end
SurveillanceCameras: false :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: false :end
KeyLockOnDoor: false :end
CipherLockOnDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: false :end
Order: 0 :end
PermittedUsers: *.Public :end
ULC: 33 49 :end
LRC: 56 31 :end
DoorGuardPosX: 48 :end
DoorGuardPosY: 33 :end
DoorGuardFacing: EAST :end

:end //of Zone

Zone:
Name: lower right :end
Description: :end
Site: Main Site :end
Art: 3aLR.tga :end
Static: false :end
StaticSelectable: false :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
// Start Default Component Settings
HoldsUserAsset: true :end
ProtectWithACL: true :end
WriteDownPasswords: true :end
LockorLogoff: false :end
PasswordLength: short :end
PasswordCharacterSet: any :end
PasswordChangeFrequency: never :end
NoEmailAttachmentExecute: false :end
NoExternalSoftware: false :end
NoUseOfModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: false :end
ApplyPatches: false :end
LeaveMachinesOn: false :end
NoPhysicalModifications: false :end
UserBackup: false :end

```
        // End Default Component Settings
        Receptionist: false :end
        GuardAtDoor: false :end
        PatrollingGuard: false :end
        ProhibitMedia: false :end
        ProhibitPhoneDevices: false :end
        ExpensivePerimeterAlarms: false :end
        ModeratePerimeterAlarms: false :end
        Re-enforcedWalls: false :end
        SurveillanceCameras: false :end
        PermitEscortedVisitors: false :end
        VisualPeopleInspection: false :end
        XrayPackages: false :end
        KeyLockOnDoor: false :end
        CipherLockOnDoor: false :end
        ExpensiveIrisScanner: false :end
        ModerateIrisScanner: false :end
        Badges: false :end
        Order: 0 :end
        PermittedUsers: *.Public :end
        ULC:  50 41 :end
        LRC:  56 31 :end
        DoorGuardPosX: 50 :end
        DoorGuardPosY: 38 :end
        DoorGuardFacing: NORTH :end
:end //of Zone

Zone:
        Name: upper right :end
        Description:  :end
        Site: Main Site :end
        Art: 3aUR.tga :end
        Static: false :end
        StaticSelectable: false :end
        RemoteAuthentication: false :end
        AcceptPKICerts: false :end
        UseOneTimePasswordToken: false :end
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
        UseClientPKICerts: false :end
        VPNClient: false :end
        ScanEmailAttachments: false :end
        StripEmailAttachments: false :end
        AutomaticLockLogout: false :end
        SelfAdminister: false :end
        SelfAdministerMAC: false :end
```

UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
// Start Default Component Settings
HoldsUserAsset: true :end
ProtectWithACL: true :end
WriteDownPasswords: true :end
LockorLogoff: false :end
PasswordLength: short :end
PasswordCharacterSet: any :end
PasswordChangeFrequency: never :end
NoEmailAttachmentExecute: false :end
NoExternalSoftware: false :end
NoUseOfModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: false :end
ApplyPatches: false :end
LeaveMachinesOn: false :end
NoPhysicalModifications: false :end
UserBackup: false :end
// End Default Component Settings
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: true :end
ModeratePerimeterAlarms: false :end
Re-enforcedWalls: true :end
SurveillanceCameras: false :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: false :end
KeyLockOnDoor: true :end
CipherLockOnDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: true :end
Order: 0 :end
PermittedUsers: *.Public :end
ULC: 50 49 :end

```
        LRC:  56 42 :end
        DoorGuardPosX: 52 :end
        DoorGuardPosY: 42 :end
        DoorGuardFacing: NORTH :end
:end //of Zone

Zone:
        Name: Offsite :end
        Description:  :end
        Site: Simple Office :end
        Art: nothing.tga :end
        Static: true :end
        StaticSelectable: false :end
        RemoteAuthentication: false :end
        AcceptPKICerts: false :end
        UseOneTimePasswordToken: false :end
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
        UseClientPKICerts: false :end
        VPNClient: false :end
        ScanEmailAttachments: false :end
        StripEmailAttachments: false :end
        AutomaticLockLogout: false :end
        SelfAdminister: false :end
        SelfAdministerMAC: false :end
        UserRunsPrivileged: false :end
        BlockRemovableMedia: false :end
        EnforcePasswordPolicy: false :end
        BlockLocalStorage: false :end
        BrowserSettings: Loose :end
        EmailSettings: Loose :end
        UpdatePatches: None :end
        ManagedAntivirus: false :end
        // Start Default Component Settings
                HoldsUserAsset: true :end
                ProtectWithACL: true :end
                WriteDownPasswords: false :end
                LockorLogoff: true :end
                PasswordLength: medium :end
                PasswordCharacterSet: any :end
                PasswordChangeFrequency: never :end
                NoEmailAttachmentExecute: false :end
                NoExternalSoftware: false :end
                NoUseOfModems: false :end
                NoWebMail: true :end
                NoMediaLeaveZone: false :end
```

```
                ApplyPatches: true :end
                LeaveMachinesOn: false :end
                NoPhysicalModifications: true :end
                UserBackup: false :end
        // End Default Component Settings
        Receptionist: true :end
        GuardAtDoor: false :end
        PatrollingGuard: false :end
        ProhibitMedia: false :end
        ProhibitPhoneDevices: false :end
        ExpensivePerimeterAlarms: true :end
        ModeratePerimeterAlarms: false :end
        Re-enforcedWalls: true :end
        SurveillanceCameras: true :end
        PermitEscortedVisitors: false :end
        VisualPeopleInspection: false :end
        XrayPackages: false :end
        KeyLockOnDoor: true :end
        CipherLockOnDoor: true :end
        ExpensiveIrisScanner: false :end
        ModerateIrisScanner: true :end
        Badges: true :end
        Order: 0 :end
        PermittedUsers: *.Public :end
        ULC:  94 29 :end
        LRC:  106 21 :end
        DoorGuardFacing: NORTH :end
:end //of Zone

Secrecy:
        Name: Secret :end
        Description:  :end
        Level: 32 :end
        Category: 3 :end
        SecrecyValue: 500 :end
        SecrecyValueChange: +20 :end
        AttackerValue: 1500 :end
        AttackerValueChange: +20 :end
        InitialBackGroundCheck: Medium :end
:end //of Secrecy

Secrecy:
        Name: TopSecret :end
        Description:  :end
        Level: 48 :end
        Category: 4 :end
```

```
        SecrecyValue: 3500 :end
        SecrecyValueChange: +50 :end
        AttackerValue: 4500 :end
        AttackerValueChange: +50 :end
        InitialBackGroundCheck: High :end
:end //of Secrecy

Secrecy:
        Name: Unclassified :end
        Description:  :end
        Level: 5 :end
        Category: 1 :end
        SecrecyValue: 25 :end
        SecrecyValueChange: +10 :end
        AttackerValue: 19 :end
        AttackerValueChange: +10 :end
        InitialBackGroundCheck: None :end
:end //of Secrecy

DACGroups:
        Group: admin :end
        InitialBackGroundCheck: High :end
        Group: Operations :end
        InitialBackGroundCheck: Medium :end
:end // of DAC Groups
Asset:
        Name: PersonnelDB :end
        Description: This is the command's personnel database. It contains
personal information on everyone in the command. :end
        IsInstantiated: true :end
        HasDAC: true :end
        Secrecy: Unclassified :end
        DOSMotive: 0 :end
        AvailabilityPenalty: 0 :end
        AccessList:
                *.admin YYYY
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 100 :end
                AttackerMotive: 80 :end
        :end
:end //of Asset

Asset:
```

```
        Name: Muster Reports :end
        Description: These are the Muster reports that lists the location of
everyone in the command, including those not present at work. :end
        IsInstantiated: true :end
        HasDAC: true :end
        Secrecy: Unclassified :end
        DOSMotive: 0 :end
        AvailabilityPenalty: 0 :end
        AccessList:
                *.Operations YYYY            *.admin YYYY
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYYY :end
                Cost: 100 :end
                AttackerMotive: 40 :end
        :end
:end //of Asset

Asset:
        Name: OperationsPlans :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
        Secrecy: Unclassified :end
        DOSMotive: 150 :end
        AvailabilityPenalty: 0 :end
        AccessList:
                *.Operations YYNY
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYYY :end
                Cost: 125 :end
                AttackerMotive: 78 :end
        :end
:end //of Asset

Asset:
        Name: Command Picnic Pictures :end
        Description: These are the pictures from the command picnic. Captain
Ahab wanted them put on the LAN so everyone has access to them. :end
        IsInstantiated: false :end
        HasDAC: false :end
        Secrecy: Unclassified :end
        DOSMotive: 0 :end
```

```
        AvailabilityPenalty: 0 :end
        AccessList:
                *.Public YYYY
        :end
        CostList:
                Access: ChiefGoat :end
                AccessMode: YYYY :end
                Cost: 1 :end
                AttackerMotive: 0 :end
        :end
:end //of Asset

AssetGoal:
        Name: DBProtected :end
        Description: Protect the Personnel Database with an access control list.
:end
        Shared: true :end
        UseAssignedComputers: true :end
        Asset:
                Name: PersonnelDB :end
                filtered: false :end
                AccessMode: YYYY :end
        :end
        AvailabilityCostPenalty: 25 :end
:end //of AssetGoal

AssetGoal:
        Name: Muster Reports Avail :end
        Description:  :end
        Shared: false :end
        Asset:
                Name: Muster Reports :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 0 :end
:end //of AssetGoal

AssetGoal:
        Name: opplans :end
        Description:  :end
        Shared: false :end
        Asset:
                Name: OperationsPlans :end
                filtered: false :end
                AccessMode: YXXX :end
```

```
        :end
        AvailabilityCostPenalty: 0 :end
:end //of AssetGoal

AssetGoal:
        Name: cmdpics :end
        Description:  :end
        Shared: false :end
        AvailabilityCostPenalty: 0 :end
:end //of AssetGoal

User:
        Name: BobtheContractor :end
        Dept:  contractor :end
        SecrecyClearance:  Unclassified :end
        DefaultDAC: PUBLIC :end
        Trustworthiness:  10 :end
        InitialTraining: 55 :end
        Happiness: 55 :end
        Productivity: 95 :end
        HISupportSkill: 99 :end
        PosIndex: 2 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: Bob is a contractor that works at the shipyard. :end
:end //of User

User:
        Name: EnsignPulver :end
        Dept:  supply :end
        SecrecyClearance:  Secret :end
        DefaultDAC:  :end
        AssetGoal:
                AssetGoalName: DBProtected :end
                TargetUsage: 0 :end
                Happiness: 0 :end
                Productivity: 0 :end
        :end
        Trustworthiness:  75 :end
        InitialTraining: 5 :end
        Happiness: 99 :end
        Productivity: 10 :end
        HISupportSkill: 2 :end
        PosIndex: 7 :end
        Cost: 0 :end
        Gender: male :end
```

UserDescription: Ensign Pulver works as the Laundry and Morale Officer
:end
:end //of User

User:
Name: ChiefGoat :end
Dept: Ops :end
SecrecyClearance: Secret :end
DACGroups:
Operations :end
:end
DefaultDAC: Operations :end
Trustworthiness: 78 :end
InitialTraining: 34 :end
Happiness: 3 :end
Productivity: 95 :end
HISupportSkill: 80 :end
PosIndex: 1 :end
Cost: 0 :end
Gender: male :end
UserDescription: Chief Goat works on the file server alot. He likes to work back there because not very many people normally have physical access there.
:end
:end //of User

User:
Name: LtSmith :end
Dept: Admin :end
SecrecyClearance: TopSecret :end
DACGroups:
admin :end
:end
DefaultDAC: admin :end
AssetGoal:
AssetGoalName: DBProtected :end
TargetUsage: 0 :end
Happiness: 0 :end
Productivity: 0 :end
:end
Trustworthiness: 90 :end
InitialTraining: 55 :end
Happiness: 75 :end
Productivity: 95 :end
HISupportSkill: 90 :end
PosIndex: 4 :end
Cost: 1200 :end

```
        Gender: female :end
        UserDescription: LT Smith is the Admin Officer :end
:end //of User

User:
        Name: PettyOfficerPrice :end
        Dept:  Ops :end
        SecrecyClearance:  Secret :end
        DACGroups:
                Operations :end
        :end
        DefaultDAC: Operations :end
        Trustworthiness:  90 :end
        InitialTraining: 100 :end
        Happiness: 70 :end
        Productivity: 100 :end
        HISupportSkill: 50 :end
        PosIndex: 3 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription:  :end
:end //of User

User:
        Name: SeamanJones :end
        Dept:  Admin :end
        SecrecyClearance:  Secret :end
        DACGroups:
                admin :end
        :end
        DefaultDAC: admin :end
        AssetGoal:
                AssetGoalName: DBProtected :end
                TargetUsage: 0 :end
                Happiness: 0 :end
                Productivity: 0 :end
        :end
        Trustworthiness:  72 :end
        InitialTraining: 23 :end
        Happiness: 89 :end
        Productivity: 95 :end
        HISupportSkill: 10 :end
        PosIndex: 5 :end
        Cost: 0 :end
        Gender: male :end
```

UserDescription: Seaman Jones works in the Admin Dept with Lt Smith
:end
:end //of User

User: //SupportStaff
Name: EnsWebster :end
Dept: Tech :end
HWSupportSkill: 80 :end
SWSupportSkill: 80 :end
HISupportSkill: 50 :end
Trustworthiness: 90 :end
InitialTraining: 50 :end
Happiness: 95 :end
Productivity: 50 :end
Skill: 80 :end
PosIndex: 1 :end
Cost: 50 :end
Gender: male :end
UserDescription: Ensign Webster is the ADP officer :end
:end //of SupportStaff

User: //SupportStaff
Name: LtRoberts :end
Dept: Security :end
HWSupportSkill: 50 :end
SWSupportSkill: 50 :end
HISupportSkill: 99 :end
DaysTillAvailable: 0 :end
Trustworthiness: 90 :end
InitialTraining: 90 :end
Happiness: 80 :end
Productivity: 80 :end
Skill: 99 :end
PosIndex: 0 :end
Cost: 4000 :end
Gender: male :end
UserDescription: LT Roberts is the Duty Officer. As such, he is
responsible for enforcing the Organization's Security Policy. :end
:end //of SupportStaff

Workspace:
PosIndex: 1 :end
Type: Server :end
:end

Workspace:

PosIndex: 3 :end
:end

Workspace:
PosIndex: 4 :end
:end

Workspace:
PosIndex: 5 :end
:end

Component: //start of the physical component section.
Name: FileServer :end
IsTemplate: false :end
Description: This server stores files for use on the Local Area Network...
:end
AssetProtection: false :end
HW: Blato Server :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: ChiefGoat :end
PosIndex: 1 :end

```
        Assets: Muster Reports :end
        Assets: Command Picnic Pictures :end
        Assets: OperationsPlans :end
        AccessListLocal: *.Public :end
        AccessListRemote: *.Public :end
        UninterruptiblePower: false :end
        //NetworkConnections:
        Network:
                Name: LocalAreaNetwork :end
        :end    //end of NetworkConnections:
        ComponentProceduralSettings:
                HoldsUserAsset: false :end
                ProtectWithACL: true :end
                WriteDownPasswords: true :end
                LockorLogoff: false :end
                PasswordLength: none :end
                PasswordCharacterSet: any :end
                PasswordChangeFrequency: never :end
                NoEmailAttachmentExecute: true :end
                NoExternalSoftware: true :end
                NoUseOfModems: true :end
                NoWebMail: true :end
                NoMediaLeaveZone: true :end
                UpdateAntiVirus: Automatic :end
                ApplyPatches: false :end
                LeaveMachinesOn: true :end
                NoPhysicalModifications: true :end
                UserBackup: true :end
        :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
        Name: internetrouter :end
        IsTemplate: false :end
        Description:  :end
        AssetProtection: false :end
        HW: Bit Flipper :end
        Cost: 0 :end
        Resale: 0 :end
        Maintenance: 0 :end
        Availability: 99 :end
        Static: false :end
        OS: FlipOS :end
        RemoteAuthentication: false :end
        AcceptPKICerts: false :end
        UseOneTimePasswordToken: false :end
```

```
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
        UseClientPKICerts: false :end
        VPNClient: false :end
        ScanEmailAttachments: false :end
        StripEmailAttachments: false :end
        AutomaticLockLogout: false :end
        SelfAdminister: false :end
        SelfAdministerMAC: false :end
        UserRunsPrivileged: false :end
        BlockRemovableMedia: false :end
        EnforcePasswordPolicy: false :end
        BlockLocalStorage: false :end
        BrowserSettings: Loose :end
        EmailSettings: Loose :end
        UpdatePatches: None :end
        ManagedAntivirus: false :end
        User:  :end
        PosIndex: 1 :end
        UninterruptiblePower: false :end
        //NetworkConnections:
        Network:
                Name: Internet :end
        :end    //end of NetworkConnections:
        Network:
                Name: LocalAreaNetwork :end
        :end    //end of NetworkConnections:
        ComponentProceduralSettings:
                HoldsUserAsset: false :end
                ProtectWithACL: false :end
                WriteDownPasswords: false :end
                LockorLogoff: true :end
                PasswordLength: none :end
                PasswordCharacterSet: any :end
                PasswordChangeFrequency: never :end
                NoEmailAttachmentExecute: false :end
                NoExternalSoftware: false :end
                NoUseOfModems: false :end
                NoWebMail: false :end
                NoMediaLeaveZone: false :end
                ApplyPatches: false :end
                LeaveMachinesOn: false :end
                NoPhysicalModifications: false :end
                UserBackup: false :end
        :end //of ComponentProceduralSettings
:end //of physical component Section
```

Component: //start of the physical component section.
Name: OpenComputer :end
IsTemplate: false :end
Description: This is Price's computer. This is where Price gets all the work that he was contracted to do done. :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: PettyOfficerPrice :end
PosIndex: 3 :end
UninterruptiblePower: true :end
//NetworkConnections:
Network:
Name: LocalAreaNetwork :end
:end //end of NetworkConnections:
ComponentProceduralSettings:
HoldsUserAsset: false :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end

PasswordLength: medium :end
PasswordCharacterSet: moderate :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Regular :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: Jone's Box :end
IsTemplate: false :end
Description: This is the computer that Seaman Jones uses. :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
Software: Thin Man :end
Software: Populos Client :end
Software: Zone Out :end
Software: Populos SPF 30 :end
Software: Placebo :end
Software: Euphoria :end
Software: Viewpoint :end
Software: URL2U :end
Software: MatTracker :end
Software: Spread Triangle :end
Software: Word Triangle :end
Software: Palm Reader :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end

```
        VPNClient: false :end
        ScanEmailAttachments: false :end
        StripEmailAttachments: false :end
        AutomaticLockLogout: false :end
        SelfAdminister: false :end
        SelfAdministerMAC: false :end
        UserRunsPrivileged: false :end
        BlockRemovableMedia: false :end
        EnforcePasswordPolicy: false :end
        BlockLocalStorage: false :end
        BrowserSettings: Loose :end
        EmailSettings: Loose :end
        UpdatePatches: None :end
        ManagedAntivirus: false :end
        User: SeamanJones :end
        PosIndex: 5 :end
        AccessListRemote: *.admin :end
        UninterruptiblePower: true :end
        //NetworkConnections:
        Network:
                Name: LocalAreaNetwork :end
        :end    //end of NetworkConnections:
        ComponentProceduralSettings:
                HoldsUserAsset: false :end
                ProtectWithACL: true :end
                WriteDownPasswords: false :end
                LockorLogoff: true :end
                PasswordLength: medium :end
                PasswordCharacterSet: moderate :end
                PasswordChangeFrequency: six :end
                NoEmailAttachmentExecute: true :end
                NoExternalSoftware: true :end
                NoUseOfModems: true :end
                NoWebMail: true :end
                NoMediaLeaveZone: true :end
                UpdateAntiVirus: Regular :end
                ApplyPatches: false :end
                LeaveMachinesOn: true :end
                NoPhysicalModifications: true :end
                UserBackup: true :end
        :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
        Name: LT Smith's Desktop :end
        IsTemplate: false :end
```

Description: :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
Software: Palm Reader :end
Software: Thin Man :end
Software: Euphoria :end
Software: URL2U :end
Software: MatTracker :end
Software: Cell Life :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: LtSmith :end
PosIndex: 4 :end
Assets: PersonnelDB :end
AccessListLocal: LtSmith :end
AccessListLocal: SeamanJones :end
UninterruptiblePower: true :end
//NetworkConnections:
Network:
	Name: LocalAreaNetwork :end
:end	//end of NetworkConnections:
ComponentProceduralSettings:

HoldsUserAsset: false :end
ProtectWithACL: false :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: none :end
PasswordCharacterSet: any :end
PasswordChangeFrequency: never :end
NoEmailAttachmentExecute: false :end
NoExternalSoftware: false :end
NoUseOfModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: false :end
ApplyPatches: false :end
LeaveMachinesOn: false :end
NoPhysicalModifications: false :end
UserBackup: false :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the catalog component section.
Name: Blato Desktop Select :end
IsTemplate: true :end
Description: Packed with applications, memory and disk :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 1700 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
Software: WordSmyth :end
Software: Cell Life :end
Software: Internet Contemplator :end
Software: Viewpoint :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end

AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: NORMAL :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Targo Worksaver :end
IsTemplate: true :end
Description: Full suite of productivity software, adequate memory and dis.
:end
AssetProtection: false :end
HW: Targo Worksaver :end
Cost: 1700 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
Software: WordSmyth :end
Software: Cell Life :end
Software: Viewpoint :end
Software: Internet Contemplator :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Trusted Targo Worksaver :end
IsTemplate: true :end
Description: Similar to the Targo Worksaver, but includes the Trusted Populos OS. :end
AssetProtection: false :end
HW: Trusted Targo Worksaver :end
Cost: 2500 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Trusted Populos Desktop :end
Software: WordSmyth :end
Software: Cell Life :end
Software: Internet Contemplator :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: The Thin Man :end
IsTemplate: true :end
Description: A thin client intended to work with either Gossamer products or Populos Terminal Servers. :end
AssetProtection: false :end
HW: The Thin Man :end
Cost: 900 :end
Resale: 100 :end
Maintenance: 100 :end

Availability: 99 :end
OS: Populos Embedded V5 :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Green Net Client :end
IsTemplate: true :end
Description: A thin client intended to work with Gossamer products. Intended use is to connect to multiple networks of different sensitivity levels :end
AssetProtection: false :end
HW: Green Net Client :end
Cost: 3000 :end
Resale: 1000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Desktop :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end

SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Lunitos AFOS :end
IsTemplate: true :end
Description: Sleek colorful desktop machine with adequate memory and disk :end
AssetProtection: false :end
HW: Lunitos AFOS :end
Cost: 2300 :end
Resale: 300 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Lunitos Desktop :end
Software: URL2U :end
Software: Euphoria :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.

Name: Greenshade Client :end
IsTemplate: true :end
Description: High assurance client workstation having the Secure Shade Desktop O/S. :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 4200 :end
Resale: 800 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Desktop :end
Software: Word Triangle :end
Software: Spread Triangle :end
Software: URL2U :end
Software: Euphoria :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Targo Server :end
IsTemplate: true :end
Description: Full featured server with the worlds most popular operating system. :end
AssetProtection: false :end
HW: Targo Server :end
Cost: 15000 :end
Resale: 5000 :end
Maintenance: 100 :end

Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Blato Server :end
IsTemplate: true :end
Description: Full featured server with the worlds most popular operating system. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 15000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end

SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Twist Off Server :end
IsTemplate: true :end
Description: Server class machine with the Jar Lid Server O/S :end
AssetProtection: false :end
HW: Twist Off Server :end
Cost: 10000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Twister Terminal Server :end
IsTemplate: true :end

Description: Terminal server capable of presenting Jar Lid applications to thin client workstations. :end
AssetProtection: false :end
HW: Twist Off Server :end
Cost: 10000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Green Shade Server :end
IsTemplate: true :end
Description: Server class machine with the Secure Shade Server high assurance operating system :end
AssetProtection: false :end
HW: Green Shade Server :end
Cost: 80000 :end
Resale: 20000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end

UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Mail Appliance :end
IsTemplate: true :end
Description: Simple Email Server. :end
AssetProtection: false :end
HW: Targo Server :end
Cost: 5000 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end

UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Populos Letter Pusher :end
IsTemplate: true :end
Description: Email Server that rules. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 20000 :end
Resale: 8000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Web Appliance :end
IsTemplate: true :end
Description: Simple web server :end
AssetProtection: false :end
HW: Twist Off Server :end
Cost: 1500 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end

RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Populos Internet Slave :end
IsTemplate: true :end
Description: Web Server that rules the web. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 10000 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end

BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bit Flipper :end
IsTemplate: true :end
Description: High performance router :end
AssetProtection: false :end
HW: Bit Flipper :end
Cost: 150 :end
Resale: 60 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bit Flipper VPN :end
IsTemplate: true :end
Description: VPN Gateway -- another Bit Flipper product :end
AssetProtection: false :end
HW: Bit Flipper VPN :end
Cost: 200 :end

Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bent Line VPN :end
IsTemplate: true :end
Description: VPN Gateway Evaluated to EAL4+ :end
AssetProtection: false :end
HW: Bent Line VPN :end
Cost: 1500 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V8 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end

SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Green Shade VPN :end
IsTemplate: true :end
Description: VPN Gateway On a Green Shade Core :end
AssetProtection: false :end
HW: Green Shade VPN :end
Cost: 1500 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: GEOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Crack This! :end
IsTemplate: true :end

Description: Best Selling VPN Gateway :end
AssetProtection: false :end
HW: Crack This! :end
Cost: 1500 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Five Inches of Asbestos :end
IsTemplate: true :end
Description: Best selling firewall :end
AssetProtection: false :end
HW: Five Inches of Asbestos :end
Cost: 900 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end

VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bit Flipper Border :end
IsTemplate: true :end
Description: Full featured firewall :end
AssetProtection: false :end
HW: Bit Flipper Border :end
Cost: 200 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Wire Stuff :end
IsTemplate: true :end
Description: High quality hub with high reliability :end
AssetProtection: false :end
HW: Wire Stuff :end
Cost: 150 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Box with Wires :end
IsTemplate: true :end
Description: General purpose hub :end
AssetProtection: false :end
HW: Box with Wires :end
Cost: 90 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end

```
        UseOneTimePasswordToken: false :end
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
        UseClientPKICerts: false :end
        VPNClient: false :end
        ScanEmailAttachments: false :end
        StripEmailAttachments: false :end
        AutomaticLockLogout: false :end
        SelfAdminister: false :end
        SelfAdministerMAC: false :end
        AdministerSoftwareControl: false :end
        BlockRemovableMedia: false :end
        BlockLocalStorage: false :end
        BrowserSettings: LOOSE :end
        EmailSettings: LOOSE :end
        UpdatePatches: NONE :end
        UpdateAntivirus: NONE :end
:end //of catalog component Section

Conditions:
        Condition:
                Tagname: 1reg1 :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: 1reg2 :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: 2pwreg :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: phs2write :end
                ConditionClass: AssetComputerHasPolicy :end
                ConditionText: Muster Reports :end
                SecondConditionText:  WriteDownPassword: :end
:end //of Condition

        Condition:
                Tagname: 3attch :end
                ConditionClass: AssetComputerHasPolicy :end
                ConditionText: PersonnelDB :end
```

```
            SecondConditionText:  NoEmailAttachmentExecute: :end
:end //of Condition

        Condition:
            Tagname: 3malreg :end
            ConditionClass: Register :end
:end //of Condition

        Condition:
            Tagname: 3avupd :end
            ConditionClass: AssetComputerHasPolicy :end
            ConditionText: PersonnelDB :end
            SecondConditionText:  UpdateAntivirus:Automatic :end
:end //of Condition

        Condition:
            Tagname: 3extsw :end
            ConditionClass: AssetComputerHasPolicy :end
            ConditionText: PersonnelDB :end
            SecondConditionText:  NoExternalSoftware: :end
:end //of Condition

        Condition:
            Tagname: 3lcklgff :end
            ConditionClass: AssetComputerHasPolicy :end
            ConditionText: Muster Reports :end
            SecondConditionText:  LockorLogoff: :end
:end //of Condition

        Condition:
            Tagname: 3lcklgffreg :end
            ConditionClass: Register :end
:end //of Condition

        Condition:
            Tagname: 3regavupd :end
            ConditionClass: AssetComputerHasPolicy :end
            ConditionText: PersonnelDB :end
            SecondConditionText:  UpdateAntivirus:Regular :end
:end //of Condition

        Condition:
            Tagname: 4MediaLeaveZone :end
            ConditionClass: AssetComputerHasPolicy :end
            ConditionText: PersonnelDB :end
            SecondConditionText:  NoMediaLeaveZone: :end
```

```
:end //of Condition

        Condition:
                Tagname: 4mediareg2 :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: 4mediareg :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: 5PhySecLevel :end
                ConditionClass: ZoneHasSecurityValue :end
                ConditionText: Entire Office :end
                Parameter: 300 :end
                Parameter: 1000 :end
:end //of Condition

        Condition:
                Tagname: 5physecreg :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: 5physsecattack :end
                ConditionClass: AssetAttacked :end
                ConditionText: Muster Reports :end
                Parameter: 18 :end
                Parameter: 10 :end
                Parameter: 100 :end
:end //of Condition

        Condition:
                Tagname: 5physsecattack2 :end
                ConditionClass: AssetAttacked :end
                ConditionText: Muster Reports :end
                Parameter: 11 :end
                Parameter: 10 :end
                Parameter: 100 :end
:end //of Condition

        Condition:
                Tagname: dbattack :end
                ConditionClass: AssetAttacked :end
```

```
            ConditionText: PersonnelDB :end
            Parameter: 17 :end
            Parameter: 79 :end
            Parameter: 81 :end
:end //of Condition

    Condition:
            Tagname: dbdone :end
            ConditionClass: AssignedComputerHas :end
            ConditionText: LtSmith :end
            SecondConditionText:  ProtectWithACL: :end
:end //of Condition

    Condition:
            Tagname: dbq1y :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: dbq1Y :end
:end //of Condition

    Condition:
            Tagname: dbq1n :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: Dbq1N :end
:end //of Condition

    Condition:
            Tagname: dbq2y :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: dbq2Y :end
:end //of Condition

    Condition:
            Tagname: dbq2n :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: dbq2N :end
:end //of Condition

    Condition:
            Tagname: malmsg :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: 3malmsg :end
:end //of Condition

    Condition:
            Tagname: medialvmsg :end
            ConditionClass: TriggerGoneOff :end
```

```
            ConditionText: 4mediamsgq :end
:end //of Condition

        Condition:
            Tagname: pyssecmsg :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: 5physecmsgq :end
:end //of Condition

        Condition:
            Tagname: medialvmsg2 :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: 4medlvq :end
:end //of Condition

        Condition:
            Tagname: EndPHS2 :end
            ConditionClass: PhaseCompleted :end
            ConditionText: 2 :end
:end //of Condition

        Condition:
            Tagname: gmepaused :end
            ConditionClass: GameStateInfo :end
            Parameter: 1 :end
:end //of Condition

        Condition:
            Tagname: ZeroCash :end
            ConditionClass: MinCashOnHand :end
            Parameter: 0 :end
:end //of Condition

        Condition:
            Tagname: malobjcomp :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: 3malobj :end
:end //of Condition

        Condition:
            Tagname: malwareattack :end
            ConditionClass: AssetAttacked :end
            ConditionText: PersonnelDB :end
            Parameter: 8 :end
            Parameter: 10 :end
            Parameter: 100 :end
```

```
:end //of Condition

        Condition:
                Tagname: viruscosttrig :end
                ConditionClass: TriggerGoneOff :end
                ConditionText: viruscost :end
:end //of Condition

        Condition:
                Tagname: moviereg :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: onscrn :end
                ConditionClass: GameOnScreen :end
                Parameter: 2 :end
:end //of Condition

        Condition:
                Tagname: pwattack :end
                ConditionClass: AssetAttacked :end
                ConditionText: Muster Reports :end
                Parameter: 7 :end
                Parameter: 38 :end
                Parameter: 42 :end
:end //of Condition

        Condition:
                Tagname: pwobjcomp :end
                ConditionClass: ObjectiveCompleted :end
                ConditionText: PWobj :end
:end //of Condition

        Condition:
                Tagname: register1 :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: register2 :end
                ConditionClass: Register :end
:end //of Condition

        Condition:
                Tagname: register3 :end
```

```
            ConditionClass: Register :end
:end //of Condition

        Condition:
            Tagname: register4 :end
            ConditionClass: Register :end
:end //of Condition

        Condition:
            Tagname: soceng1 :end
            ConditionClass: Register :end
:end //of Condition

        Condition:
            Tagname: soceng2 :end
            ConditionClass: Register :end
:end //of Condition

        Condition:
            Tagname: socengfbtrig :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: socengfb :end
:end //of Condition

        Condition:
            Tagname: socengattack :end
            ConditionClass: AssetAttacked :end
            ConditionText: PersonnelDB :end
            Parameter: 13 :end
            Parameter: 10 :end
            Parameter: 100 :end
:end //of Condition

        Condition:
            Tagname: staggertip :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: unpausegametip :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

        Condition:
            Tagname: staggerobjtip :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: objtip :end
            Parameter: 1 :end
```

```
            Parameter: 1 :end
:end //of Condition

        Condition:
            Tagname: Startphs2 :end
            ConditionClass: PhaseCompleted :end
            ConditionText: 1 :end
:end //of Condition

        Condition:
            Tagname: startphs4 :end
            ConditionClass: PhaseCompleted :end
            ConditionText: 3 :end
:end //of Condition

        Condition:
            Tagname: StartPhs5 :end
            ConditionClass: PhaseCompleted :end
            ConditionText: 4 :end
:end //of Condition

        Condition:
            Tagname: time1 :end
            ConditionClass: TimeCondition :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

        Condition:
            Tagname: time3 :end
            ConditionClass: TimeCondition :end
            Parameter: 3 :end
            Parameter: 1 :end
:end //of Condition

        Condition:
            Tagname: virus :end
            ConditionClass: VirusPresent :end
:end //of Condition

:end
Triggers:
        Trigger:
            TriggerName: 2wrt :end
            TriggerClass: SetObjectiveStatus :end
            FrequencyInDays: 999 :end
```

FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: phs2write and Startphs2 :end
TriggerText: pwobj :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: bobfindsgoatpw :end
TriggerClass: SetUserThought :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: Startphs2 and_not Endphs2 :end
TriggerText: BobtheContractor :end
SecondTriggerText: Is this Chief Goat's password on this post-it note? I'll log on to his account when he leaves. :end
Parameter: 12 :end
:end //of Trigger

Trigger:
TriggerName: 2pwphscomp :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: phs2write :end
TriggerText: 3 :end
SecondTriggerText: Good Job...It is essential that all users protect their passwords. Users should not share their passwords even with people they trust!...Check your new objectives :end
:end //of Trigger

Trigger:
TriggerName: 3lcklgff :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 3lcklgff and EndPHS2 :end
TriggerText: lckcomp :end
Parameter: 1 :end

:end //of Trigger

Trigger:
TriggerName: 3lcklgffspeak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 3lcklgff and EndPHS2 :end
TriggerText: ChiefGoat :end
SecondTriggerText: I'm glad I have to lock the computer when I leave it now. I was getting tired of getting in trouble when others used my account. :end
:end //of Trigger

Trigger:
TriggerName: 3lcklgffmsg :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 3lcklgff and EndPHS2 :end
TriggerText: You should always lock or logoff your computer when you are not using it. If you don't, you leave the computer network open to attack and you may undermine various auditing mechanisms in the system. :end
:end //of Trigger

Trigger:
TriggerName: 3malobj :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: EndPHS2 and 3attch and 3extsw and (3avupd or 3regavupd) :end
TriggerText: malware :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: malobjsmithtalk :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end

FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: EndPHS2 and 3attch and 3extsw and (3avupd or 3regavupd) :end
TriggerText: LtSmith :end
SecondTriggerText: I'm glad I did not open that Virus-laden Program that Mom sent me in an email. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: 3malmsg :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: EndPHS2 and 3attch and 3extsw and (3avupd or 3regavupd) :end
TriggerText: Malicious Software comes in many forms. For information press 'e' and read the malicious software tutorial in the encyclopedia. :end
:end //of Trigger

Trigger:
TriggerName: 3phs :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: EndPHS2 and 3lcklgff and 3attch and 3extsw and (3regavupd or 3avupd) :end
TriggerText: 4 :end
:end //of Trigger

Trigger:
TriggerName: 4MediaLvZone :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 4MediaLeaveZone and startphs4 :end
TriggerText: SmithMediaLvZne :end

Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: 4medlvq :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 4MediaLeaveZone and startphs4 :end
TriggerText: False Alarm. LT Smith was stopping at the vault on her way home to store the Personnel Database backup offsite just in a disaster destroyed the office(like a fire). :end
:end //of Trigger

Trigger:
TriggerName: 4mediamsgq :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 4MediaLeaveZone and startphs4 :end
TriggerText: It is essential to backup data. Backups should be securely stored off-site or if that is not possible physically separated from the computer system. This will ensure availability and easy recovery during various contingencies. Appropriate safeguards should be applied to backups to ensure their confidentiality, integrity, and availabilty. :end
:end //of Trigger

Trigger:
TriggerName: 4phscomp :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: startphs4 and 4MediaLeaveZone :end
ConditionParameter3: n :end
ConditionParameter4: y :end
TriggerText: 5 :end
:end //of Trigger

Trigger:
TriggerName: 5PhySecObj :end

TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: StartPhs5 AND 5PhySecLevel :end
TriggerText: PhySec :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: 5physecmsgq :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: StartPhs5 AND 5PhySecLevel :end
ConditionParameter2: n :end
ConditionParameter3: y :end
TriggerText: There are many ways to improve the physical security of an organization. One of the most important can be achieved by all employees, that is vigilance. When employees see suspicious activity, report it. If you don't know who to report it to, start with your boss. :end
:end //of Trigger

Trigger:
TriggerName: 5physecwin :end
TriggerClass: WinTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: StartPhs5 AND 5PhySecLevel :end
TriggerText: The entire office is protected with a reasonable amount of physical security to mitigate the risks. You have completed this training scenario. Well done! (PARAGRAPH) To learn more, try the advanced user training. In that scenario, you will connect computers to the Siprnet and Niprnet, learn about filtering rules, set security policy, and defend against some more sophisticated attacks. :end
:end //of Trigger

Trigger:
TriggerName: insiderdb :end
TriggerClass: AttackTrigger :end
FrequencyInDays: .05 :end

FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: time1 AND_NOT dbdone :end
TriggerText: dbattack :end
Parameter: 17 :end
Parameter: -2 :end
:end //of Trigger

Trigger:
TriggerName: dbattackticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: dbattack :end
TriggerText: An untrusted user is trying to gain access to assets he does not have access to. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: pwattack :end
TriggerClass: AttackTrigger :end
FrequencyInDays: .05 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: time1 and Startphs2 AND_NOT phs2write AND_NOT EndPHS2 :end
TriggerText: pwattack :end
Parameter: 7 :end
Parameter: -2 :end
:end //of Trigger

Trigger:
TriggerName: pwattackticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: pwattack :end
TriggerText: Bad users are doing bad things using passwords they shouldn't have. :end

Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: 5physsecattack :end
TriggerClass: AttackTrigger :end
FrequencyInDays: .05 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: time1 AND Startphs5 AND_NOT 5PhySecLevel AND_NOT time3 :end
TriggerText: 5physsecattack :end
Parameter: 18 :end
Parameter: -2 :end
:end //of Trigger

Trigger:
TriggerName: 5physsecattackticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: 5physsecattack :end
TriggerText: Why is there an outsider breaking in to get assets? :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: 5physsecattack2 :end
TriggerClass: AttackTrigger :end
FrequencyInDays: .04 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: time3 AND Startphs5 AND_NOT 5PhySecLevel :end
TriggerText: 5physsecattack2 :end
Parameter: 11 :end
Parameter: -2 :end
:end //of Trigger

Trigger:
TriggerName: 5physsecattack2ticker :end
TriggerClass: TickerTrigger :end

FrequencyInDays: 1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: time3 AND Startphs5 AND_NOT 5PhySecLevel :end
TriggerText: Someone has broken in and is going to steal your hardware. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: 3malwareattack :end
TriggerClass: AttackTrigger :end
FrequencyInDays: .05 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: time1 AND EndPHS2 AND_NOT startphs4 :end
TriggerText: malwareattack :end
Parameter: 8 :end
Parameter: -2 :end
:end //of Trigger

Trigger:
TriggerName: 3malwareattackticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .5 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: malwareattack AND_NOT startphs4 :end
TriggerText: Some of your assets are being targeted with malicious software. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: socengattack :end
TriggerClass: AttackTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: soceng1 AND EndPHS2 AND_NOT StartPhs5 AND (soceng2 or soceng2) :end
ConditionParameter1: y :end

ConditionParameter4: y :end
ConditionParameter5: n :end
TriggerText: socengattack :end
Parameter: 13 :end
Parameter: -2 :end
:end //of Trigger

Trigger:
TriggerName: socengattackticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: soceng1 AND EndPHS2 AND_NOT StartPhs5 AND (soceng2 or soceng2) :end
ConditionParameter1: y :end
ConditionParameter4: y :end
ConditionParameter5: n :end
TriggerText: An intruder broke in using Ensign Pulver's ID and special kowledge he learned from you on the phone. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: bobtalk :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: .02 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: Startphs2 :end
TriggerText: BobTheContractor :end
SecondTriggerText: I'm Bob. I'm a contractor from the shipyard. I have access to this whole place. I bet they didn't even do a background check on me. :end
:end //of Trigger

Trigger:
TriggerName: dbquiz :end
TriggerClass: Question :end
FrequencyInDays: .01 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end

ConditionList: dbdone AND_NOT register1 AND_NOT register1 :end
ConditionParameter2: y :end
ConditionParameter3: n :end
TriggerText: Good Job. now for a quick quiz. Do you think that a Database with personal information should be accessible by all members of the command? Press Y or N and then click OK :end
SecondTriggerText: register1 :end
:end //of Trigger

Trigger:
TriggerName: dbq1Y :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: register1 :end
ConditionParameter1: y :end
TriggerText: Think again. A personnel Database should be protected against unauthorized disclosure. Private information of people in your organization must be appropriately safeguarded and used only for official business. Protecting information that may be in a personnel database may be required by the Privacy Act. :end
:end //of Trigger

Trigger:
TriggerName: Dbq1N :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: register1 :end
ConditionParameter1: n :end
TriggerText: Correct, you should protect a personnel database. Not only should private information be safeguarded and used only for official business, but it is federal law under the Privacy Act to do so. :end
:end //of Trigger

Trigger:
TriggerName: dbq2 :end
TriggerClass: Question :end
FrequencyInDays: .01 :end
FixedDelay: 0 :end
RandomDelay: 0 :end

RunsWhilePaused: false :end
ConditionList: register1 OR register1 AND_NOT register3 AND_NOT register3 :end
ConditionParameter1: y :end
ConditionParameter2: n :end
ConditionParameter3: y :end
ConditionParameter4: n :end
TriggerText: Do you think that a folder with pictures from the command picnic should be available for everyone in the Command? Press Y or N and then click OK. :end
SecondTriggerText: register3 :end
:end //of Trigger

Trigger:
TriggerName: dbq2Y :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: register3 :end
ConditionParameter1: y :end
TriggerText: Correct, pictures from a command picnic should be shared with all members of the Command. Information of this type should be available to everyone in the organization and contributes to good morale in the workplace. :end
:end //of Trigger

Trigger:
TriggerName: dbq2N :end
TriggerClass: MessageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: register3 :end
ConditionParameter1: n :end
TriggerText: Think about it. Pictures from a command picnic should be available to all members of the Command. Information of this type contributes to good morale in the workplace. :end
:end //of Trigger

Trigger:
TriggerName: soceng1 :end
TriggerClass: Question :end
FrequencyInDays: .01 :end

FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: register3 OR register3 AND_NOT soceng1 AND_NOT soceng1 :end
ConditionParameter1: y :end
ConditionParameter2: n :end
ConditionParameter3: y :end
ConditionParameter4: n :end
TriggerText: Bob Woodstein called to interview you for some background for his next book. He said that he talked to Captain Ahab about it after he read about your command picnic in the base newspaper. Will you give him enough time out of your busy schedule to answer a few questions so that your command can finally get some good publicity?(Press y or n and then click OK) :end
SecondTriggerText: soceng1 :end
:end //of Trigger

Trigger:
TriggerName: dbobj :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: soceng1 OR soceng1 :end
ConditionParameter1: y :end
ConditionParameter2: n :end
TriggerText: DB has ACL :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: socengfb :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: soceng1 OR soceng1 :end
ConditionParameter1: y :end
ConditionParameter2: n :end
TriggerText: LtRoberts :end
SecondTriggerText: Captain Ahab never permits anyone to give interviews over the phone until they you can verify their identity. :end
:end //of Trigger

Trigger:
TriggerName: phs1comp :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: .02 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: soceng1 OR soceng1 :end
ConditionParameter1: y :end
ConditionParameter2: n :end
TriggerText: 2 :end
SecondTriggerText: Click on objectives to view your new objective concerning passwords. :end
:end //of Trigger

Trigger:
TriggerName: enspulverthought :end
TriggerClass: SetUserThought :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: onscrn :end
TriggerText: EnsignPulver :end
SecondTriggerText: I wonder if Captain Ahab liked the Marbles in his overhead? :end
Parameter: 11 :end
:end //of Trigger

Trigger:
TriggerName: pulvthought2 :end
TriggerClass: SetUserThought :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: EndPHS2 :end
TriggerText: EnsignPulver :end
SecondTriggerText: Does the Duty Officer really need a shotgun with a laser sight? :end
Parameter: 12 :end
:end //of Trigger

Trigger:
TriggerName: ZeroCashLoss :end

TriggerClass: LoseTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: ZeroCash :end
TriggerText: You spent all of your money! You lose. Try again. :end
:end //of Trigger

Trigger:
TriggerName: phs1 :end
TriggerClass: ClearMalware :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: Startphs2 :end
:end //of Trigger

Trigger:
TriggerName: phs2 :end
TriggerClass: ClearMalware :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: EndPHS2 :end
:end //of Trigger

Trigger:
TriggerName: objtip :end
TriggerClass: HelpTipTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: onscrn AND staggertip :end
TriggerText: Click here to look at your objectives at any time during the game :end
Parameter: 400 :end
Parameter: 500 :end
Parameter: 820 :end
Parameter: 340 :end
:end //of Trigger

Trigger:

```
        TriggerName: phs1 :end
        TriggerClass: SaveGameTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: Startphs2 :end
        TriggerText: 1 :end
:end //of Trigger

Trigger:
        TriggerName: phs2 :end
        TriggerClass: SaveGameTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: EndPHS2 :end
        TriggerText: 2 :end
:end //of Trigger

Trigger:
        TriggerName: phs3 :end
        TriggerClass: SaveGameTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: startphs4 :end
        TriggerText: 3 :end
:end //of Trigger

Trigger:
        TriggerName: phs4 :end
        TriggerClass: SaveGameTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: StartPhs5 :end
        TriggerText: 4 :end
:end //of Trigger

Trigger:
        TriggerName: soceng :end
        TriggerClass: MessageTrigger :end
```

FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: startphs4 :end
TriggerText: Most Social Engineering attacks need some sort of combination of time, access, and special knowledge. Do you really know if Bob Woodstein was really the person you were talking to during the second phase? What kinds of things can you do to verify the identity of someone? If you cannot verify someone's identity, refer them up the chain of command or to a Public Affairs Officer. Also, does your organization have more than 1 mechanism in place to secure valuable things? What can someone who has Ensign Pulver's ID get access to? Can people on the outside of your organization get internal information easily? :end
:end //of Trigger

Trigger:
TriggerName: socengobjcomp :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: startphs4 :end
TriggerText: soceng :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: soceng2 :end
TriggerClass: Question :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: pwobjcomp :end
TriggerText: Ensign Pulver needs you to sign a request form for a new ID. He said he thinks he lost it out in town last night. He had to be escorted on base today by the base police. As acting security officer, will you sign his request so that he can get a new ID? (As a sidenote, Ensign Pulver's ID will get someone access to the entire organization) :end
SecondTriggerText: soceng2 :end
:end //of Trigger

Trigger:
TriggerName: pulveridY :end

TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: soceng2 :end
ConditionParameter1: y :end
TriggerText: EnsignPulver :end
SecondTriggerText: I wonder if someone took my old ID. :end
:end //of Trigger

Trigger:
TriggerName: pulveridN :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: soceng2 :end
ConditionParameter1: n :end
TriggerText: EnsignPulver :end
SecondTriggerText: I can't believe he wouldn't sign off on my new ID. At least now he has to wake up early to escort me to work everyday. I can't believe I lost my ID playing Charades with the Chiefs. And of course it will cost him $200. :end
:end //of Trigger

Trigger:
TriggerName: pulvernidcash :end
TriggerClass: CashTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: soceng2 :end
ConditionParameter1: n :end
Parameter: -100 :end
:end //of Trigger

Trigger:
TriggerName: socengcash :end
TriggerClass: CashTrigger :end
FrequencyInDays: 1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end

ConditionList: socengattack :end
TriggerText: Someone used Ens Pulver's ID and some special knowledge from Tom Clancy Jr to break in and get access to the personnel database :end
Parameter: -500 :end
:end //of Trigger

Trigger:
TriggerName: unpausegametip :end
TriggerClass: HelpTipTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 1 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: onscrn :end
TriggerText: Press here to start the game. :end
Parameter: 300 :end
Parameter: 400 :end
Parameter: 765 :end
Parameter: 80 :end
:end //of Trigger

Trigger:
TriggerName: IncFunds4 :end
TriggerClass: CashTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: StartPhs5 :end
Parameter: +5000 :end
:end //of Trigger

Trigger:
TriggerName: physectalk :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: StartPhs5 :end
TriggerText: EnsignPulver :end
SecondTriggerText: Captain Ahab has given you $5000 to increase the Physical Security level to 300. Check your new objectives. :end
Parameter: 1 :end
:end //of Trigger

```
        Trigger:
                TriggerName: viruscost :end
                TriggerClass: CashTrigger :end
                FrequencyInDays: 999 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: false :end
                ConditionList: virus AND EndPHS2 :end
                TriggerText: Someone installed a virus on the network. This will
cost you $300 to clean up. :end
                Parameter: -300 :end
        :end //of Trigger

        Trigger:
                TriggerName: removemalware :end
                TriggerClass: ClearMalware :end
                FrequencyInDays: 999 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: false :end
                ConditionList: viruscosttrig :end
        :end //of Trigger

:end
Phases:
Phase:
        TagName: 1 :end
        DisplayName: Protect the Personnel Database with an ACL. The
database contains sensitive information that is protected under the Privacy Act
:end
        CompletedText: You have protected the Personnel Database with an ACL
:end
        UncompletedText:  :end
        PhaseCompleted: False :end
 :end //of Phase

Phase:
        TagName: 2 :end
        DisplayName: Protect Chief Goat's password from an unescorted
contractor :end
        CompletedText: It is essential that Information System Users protect the
means by which they are authenticated to a system. :end
        UncompletedText:  :end
        PhaseCompleted: False :end
 :end //of Phase
```

Phase:
TagName: 3 :end
DisplayName: Malware prevention and Computer Security: Change the settings on LT Smith's computer and the file server :end
CompletedText: :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

Phase:
TagName: 4 :end
DisplayName: Suspicious activity and Social Engineering acceptable/ethical use of dod sys :end
CompletedText: :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

Phase:
TagName: 5 :end
DisplayName: Physical Security. After some high profile security incidents, Captain Ahab has directed that you increase the Physical Security Level to 250 :end
CompletedText: You have finished this training. :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

:end
Objectives:
Objective:
TagName: DB has ACL :end
DisplayName: :end
Phase: 0 :end
ObjectiveCompleted: false :end
LastPhase: 0 :end
CompletedText: You have just placed an ACL on the Personnel Database. It is no longer open to the world. :end
UncompletedText: Your first task will be to apply an Access Control List (ACL) to the Personnel Database in the Admin Dept. The Personnel Database is an asset that must be used only by the Admin Dept. Set the "protect with ACL" procedural setting to protect this asset with an ACL via the component tab. You should do this quickly as there might be someone who wishes to access and then disclose this information. You can find out where the Personnel Database is located via the "Asset Tab." If you would like to look at the ACL after you have

selected the proper setting, click on "ACL" on the asset list (bottom right of component screen) to look at the current file permissions. :end
:end //of Objective

Objective:
TagName: lckcomp :end
DisplayName: Security has become lax on the file server. File server users regularly leave the office with their accounts logged on and wide open. Many people have noticed, but have not said anything. Captain Ahab recently got an email from Chief Goat that Chief Goat denied sending. Help the users of the file server and change the procedural setting on the computer to force them to lock or logoff when they leave it unattended. :end
Phase: 2 :end
ObjectiveCompleted: false :end
LastPhase: 2 :end
CompletedText: Users no longer leave themselves logged on the file server. :end
UncompletedText: :end
:end //of Objective

Objective:
TagName: malware :end
DisplayName: LT Smith is new to the command. Her computer needs 3 procedural changes to get it up to the same level of protection against malicious software that other computers in the command have. Select the component tab, click on "LT Smith's Desktop," and choose the proper procedural settings.(Hint- You should regularly do something, What can be attached to an email?, and has the software been approved to operate on your system?) If you still need more help, go to the encyclopedia (use the "e" key). You will find useful information on malicious software as well as an instructional video. :end
Phase: 2 :end
ObjectiveCompleted: false :end
LastPhase: 2 :end
CompletedText: You have prevented a virus from penetrating the command through LT Smith's computer. Well done. :end
UncompletedText: A virus is on the verge of infecting the command through security holes in LT Smith's computer. What will you do? :end
:end //of Objective

Objective:
TagName: SmithMediaLvZne :end
DisplayName: LT Roberts reported to you that he saw LT Smith going home with a CD labeled "Personnel Database." Click on component and determine which procedural setting to set on LT Smith's desktop that you will use to tell LT Smith to keep government computer media at work and to not take it out of the proper zone. :end

Phase: 3 :end
ObjectiveCompleted: false :end
LastPhase: 3 :end
CompletedText: False Alarm. LT Smith was stopping at the vault on her way home to store the Personnel Database backup offsite just in a disaster destroyed the office. It is essential that only trusted personnel handle data backups. :end
UncompletedText: :end
:end //of Objective

Objective:
TagName: PhySec :end
DisplayName: After several questionable incidents that were reported to the Captain through the Security Manager, Captain Ahab has given you $5000 to increase the level of physical security throughout the entire office to 300. Click on the "zone" tab and peruse the physical security options on the lower left hand portion of the screen. Buy various mechanisms to improve the physical security level throughout the entire office. Be careful not to go broke, otherwise you will lose the game and have to start over. :end
Phase: 4 :end
ObjectiveCompleted: false :end
LastPhase: 4 :end
CompletedText: You have increased the physical security to an acceptable level through various controls such as patrolling guards, badges, escorting visitors, cipher locks, locks, iris scanners, etc. :end
UncompletedText: :end
:end //of Objective

Objective:
TagName: PWobj :end
DisplayName: Chief Goat left his password written down on a post-it note on the file server. Unbelievably, this procedure is currently allowed on the file server! Click on the component tab, find the file server, and uncheck the ”allow writing passwords” procedural setting to correct this. You must do this before an untrustworthy person uses this password to maliciously use the system. :end
Phase: 1 :end
ObjectiveCompleted: false :end
LastPhase: 1 :end
CompletedText: You have completed the Password obj :end
UncompletedText: :end
:end //of Objective

Objective:
TagName: soceng :end
DisplayName: Social Engineering is a term used by security professionals that describes a technique by which an attacker uses deception or persuasion to

gain access to an information system. Typically, a social engineer needs a combination of time, special knowledge, and access to successfully infiltrate an information system. Your objective is to prevent a successful social engineering attack from occurring during this scenario. :end
Phase: 1 :end
ObjectiveCompleted: false :end
LastPhase: 3 :end
CompletedText: :end
UncompletedText: :end
:end //of Objective

:end
ShortBriefing:
You have been put in charge of Information Assurance for your command. Your goal is simple: Protect your organization's computer systems by completing the objectives of the scenario. You must do this while saving the most money possible. (PARAGRAPH) You will explore situations that will examine Information Assurance principles. Click on the GAME tab for a full description of the attributes of Information Assurance. You can type 'e' at any time to bring up the CyberCIEGE encyclopedia. There you can learn how to play the game, and read or watch movies about various Information Assurance topics.
:end

Briefing:
Joint Pub 3-13 defines Information Assurance as Information Operations that protect and defend information systems by ensuring their AVAILABILITY, INTEGRITY, AUTHENTICATION, CONFIDENTIALITY, AND NONREPUDIATION. It goes further to say that this includes the restoration of information systems by incorporating protection, detection, and reaction capabilities. (PARAGRAPH) Information Assurance is comprised of five attributes. Often, when you do something that affects one attribute, it may have an effect on the others. The goal of this training is to help you understand some of the basic mechanisms of Information Assurance, how they interact, and why it is important for everyone to be familiar with and supportive of your organization's security posture. The attributes of Information Assurance are: (PARAGRAPH) Confidentiality: Protection from unauthorized disclosure (PARAGRAPH) Integrity: Protection from unauthorized change (PARAGRAPH) Availability: Assured access by authorized users (PARAGRAPH) Authentication: Verification of originator (PARAGRAPH) Nonrepudiation: Undeniable proof of participation (PARAGRAPH)
:end

:EndOfFile

APPENDIX B: TECHNICAL USER SCENARIO DEFINITION FILE

```
//FILE:iata2.CSM
//DESIGNER:nobody
SDFid: iata2.CSM 3/12/06 5 13 PM :end
Organization:
        Name: USS Ship :end
        Title: Technical User Training Scenario :end
        StartMonth: 1 :end
        StartDay: 5 :end
        StartHour: 8 :end
        StartMinute: 0 :end
        StartMoney: 300000 :end
        Budget: 0 :end
        ProfitSharing: 0 :end
        MainOfficeVersion: small :end
        OffsiteOfficeVersion: small_office :end
        WorkSpaceFile: WorkSpaceiata2.txt :end
        Internet: true :end
        InternetStatic: false :end
        EasyTraining: false :end
        EasyACLs: false :end
        AttackTickers: true :end
        TutorialAttacks: false :end
        QuitText: Qutting Already? :end
:end //of Organization

Site:
        Name: USS Ship :end
:end  //of Site

Options:
        UseScenarioCatalogItems: YES :end
        NonServerDefaultPublicAccess: NO :end
        NetworksEverywhere: YES :end
        GuardCostsAtStartup: NO :end
:end
Camera:
        ViewCenterX: 45 :end
        ViewCenterY: 41 :end
        ViewAmountZoom: 2 :end
        ViewAmountAngle: -86 :end
:end // of Camera
```

```
AttackMasks:
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
        Mask: 1 :end
:end // of attackMask
VIEWPOINT: // overview
        FromX: 150 :end
        FromY: 100.0 :end
        FromZ: 25.0 :end
        ToX: 150.0 :end
        ToY: 0.0 :end
        ToZ: 125.0 :end
:end // Viewpoint block
VIEWPOINT: // left
        FromX: 140 :end
        FromY: 40.0 :end
        FromZ: 85.0 :end
        ToX: 100.0 :end
        ToY: 0.0 :end
        ToZ: 125.0 :end
:end // Viewpoint block
VIEWPOINT: // back
        FromX: 180 :end
        FromY: 40.0 :end
        FromZ: 125.0 :end
        ToX: 140.0 :end
        ToY: 0.0 :end
        ToZ: 145.0 :end
```

```
:end // Viewpoint block
VIEWPOINT: // center
        FromX: 140 :end
        FromY: 40.0 :end
        FromZ: 85.0 :end
        ToX: 140.0 :end
        ToY: 0.0 :end
        ToZ: 125.0 :end
:end // Viewpoint block
VIEWPOINT: // right
        FromX: 180 :end
        FromY: 70.0 :end
        FromZ: 100.0 :end
        ToX: 160.0 :end
        ToY: 0.0 :end
        ToZ: 120.0 :end
:end // Viewpoint block

Network:
        Name: NiprLan :end
        Static: false :end
:end //of Network

Network:
        Name: OffsiteNetworks :end
        Static: true :end
:end //of Network

Network:
        Name: SiprLan :end
        Static: false :end
:end //of Network

Network:
        Name: SIPRNET :end
        Static: true :end
:end //of Network

Network:
        Name: UnclassDMZ :end
        Static: false :end
:end //of Network

Department:
        Name: admin :end
:end //of Department
```

Department:
	Name: Ship'sCompany :end
:end //of Department

Department:
	Name: operations :end
:end //of Department

Department:
	Name: CommsDivision :end
:end //of Department

Zone:
	Name: Admin :end
	Description: This is where the Admin department works. :end
	Site: USS Ship :end
	Art: smallofficeupper.tga :end
	Static: false :end
	StaticSelectable: false :end
	RemoteAuthentication: false :end
	AcceptPKICerts: false :end
	UseOneTimePasswordToken: false :end
	UseBiometrics: false :end
	UseTokenPKICerts: false :end
	UseClientPKICerts: false :end
	VPNClient: false :end
	ScanEmailAttachments: false :end
	StripEmailAttachments: false :end
	AutomaticLockLogout: false :end
	SelfAdminister: false :end
	SelfAdministerMAC: false :end
	UserRunsPrivileged: false :end
	BlockRemovableMedia: false :end
	EnforcePasswordPolicy: false :end
	BlockLocalStorage: false :end
	BrowserSettings: Loose :end
	EmailSettings: Loose :end
	UpdatePatches: None :end
	ManagedAntivirus: false :end
	Receptionist: false :end
	GuardAtDoor: false :end
	PatrollingGuard: false :end
	ProhibitMedia: false :end
	ProhibitPhoneDevices: false :end
	ExpensivePerimeterAlarms: false :end

ModeratePerimeterAlarms: false :end
Re-enforcedWalls: false :end
SurveillanceCameras: false :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: false :end
KeyLockOnDoor: false :end
CipherLockOnDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: false :end
Order: 1 :end
PermittedUsers: *.Public :end
ULC: 39 58 :end
LRC: 50 44 :end
DoorGuardFacing: NORTH :end
:end //of Zone

Zone:
Name: Computer room :end
Description: This is where the Communication division works and it contains all of the networking equipment, including the servers. :end
Site: USS Ship :end
Art: smallofficeleft.tga :end
Static: false :end
StaticSelectable: false :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end

Receptionist: false :end
Guard At Door: false :end
Patrolling Guard: false :end
Prohibit Media: false :end
Prohibit Phone Devices: false :end
Expensive Perimeter Alarms: false :end
Moderate Perimeter Alarms: false :end
Re-enforced Walls: false :end
Surveillance Cameras: false :end
Permit Escorted Visitors: false :end
Visual People Inspection: false :end
Xray Packages: false :end
Key Lock On Door: false :end
Cipher Lock On Door: false :end
Expensive Iris Scanner: false :end
Moderate Iris Scanner: false :end
Badges: false :end
Order: 1 :end
Permitted Users: *.Public :end
ULC: 32 46 :end
LRC: 39 32 :end
Door Guard Facing: NORTH :end
:end //of Zone

Zone:
Name: Entire Office :end
Description: :end
Site: USS Ship :end
Art: smalloffice.tga :end
Static: false :end
Static Selectable: false :end
Remote Authentication: false :end
Accept PKI Certs: false :end
Use One Time Password Token: false :end
Use Biometrics: false :end
Use Token PKI Certs: false :end
Use Client PKI Certs: false :end
VPN Client: false :end
Scan Email Attachments: false :end
Strip Email Attachments: false :end
Automatic Lock Logout: false :end
Self Administer: false :end
Self Administer MAC: false :end
User Runs Privileged: false :end
Block Removable Media: false :end
Enforce Password Policy: false :end

BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
ModeratePerimeterAlarms: false :end
Re-enforcedWalls: false :end
SurveillanceCameras: false :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: false :end
KeyLockOnDoor: false :end
CipherLockOnDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: false :end
Order: 0 :end
PermittedUsers: *.Public :end
ULC: 32 52 :end
LRC: 58 32 :end
DoorGuardFacing: EAST :end
:end //of Zone

Zone:
Name: Operations :end
Description: This is where the Operations department works. :end
Site: USS Ship :end
Art: smallofficeright.tga :end
Static: false :end
StaticSelectable: false :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end

SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
ModeratePerimeterAlarms: false :end
Re-enforcedWalls: false :end
SurveillanceCameras: false :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: false :end
KeyLockOnDoor: false :end
CipherLockOnDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: false :end
Order: 1 :end
PermittedUsers: *.Public :end
ULC: 51 46 :end
LRC: 58 32 :end
DoorGuardFacing: NORTH :end
:end //of Zone

Zone:
Name: Offsite :end
Description: :end
Site: USS Ship :end
Art: offsitezone.tga :end
Static: true :end
StaticSelectable: false :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end

UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
// Start Default Component Settings
HoldsUserAsset: false :end
MaxSecrecyLabel: Sensitive but unclassified :end
MinSecrecyLabel: Unclassified :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: medium :end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
// End Default Component Settings
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: true :end
ModeratePerimeterAlarms: false :end
Re-enforcedWalls: false :end
SurveillanceCameras: false :end
PermitEscortedVisitors: false :end

VisualPeopleInspection: false :end
XrayPackages: false :end
KeyLockOnDoor: false :end
CipherLockOnDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: false :end
Order: 1 :end
ExcludeNetwork: SiprLan :end
ExcludeNetwork: SIPRNET :end
ExcludeNetwork: UnclassDMZ :end
ExcludeNetwork: NiprLan :end
ULC: 94 30 :end
LRC: 104 18 :end
DoorGuardFacing: NORTH :end
:end //of Zone

Secrecy:
Name: Confidential :end
Description: :end
Level: 20 :end
Category: 3 :end
SecrecyValue: 300 :end
AttackerValue: 1000 :end
InitialBackGroundCheck: Low :end
:end //of Secrecy

Secrecy:
Name: Sensitive but unclassified :end
Description: :end
Level: 16 :end
Category: 2 :end
SecrecyValue: 250 :end
SecrecyValueChange: 0 :end
AttackerValue: 750 :end
AttackerValueChange: 0 :end
InitialBackGroundCheck: None :end
:end //of Secrecy

Secrecy:
Name: Secret :end
Description: :end
Level: 32 :end
Category: 3 :end
SecrecyValue: 500 :end
SecrecyValueChange: +20 :end

```
        AttackerValue: 1500 :end
        AttackerValueChange: +20 :end
        InitialBackGroundCheck: Medium :end
:end //of Secrecy

Secrecy:
        Name: TopSecret :end
        Description:  :end
        Level: 48 :end
        Category: 4 :end
        SecrecyValue: 3500 :end
        SecrecyValueChange: +50 :end
        AttackerValue: 4500 :end
        AttackerValueChange: +50 :end
        InitialBackGroundCheck: High :end
:end //of Secrecy

Secrecy:
        Name: Unclassified :end
        Description:  :end
        Level: 5 :end
        Category: 1 :end
        SecrecyValue: 25 :end
        SecrecyValueChange: +10 :end
        AttackerValue: 19 :end
        AttackerValueChange: +10 :end
        InitialBackGroundCheck: None :end
:end //of Secrecy

DACGroups:
        Group: AdministrativeDepartment :end
        InitialBackGroundCheck: Low :end
        Group: CommunicationsDivision :end
        InitialBackGroundCheck: High :end
        Group: OperationsDepartment :end
        InitialBackGroundCheck: Medium :end
        Group: Public :end
        InitialBackGroundCheck: None :end
        Group: ShipsCompany :end
        InitialBackGroundCheck: None :end
:end // of DAC Groups
Asset:
        Name: WebResources :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
```

```
        DOSMotive: 0 :end
        AvailabilityPenalty: 0 :end
        AccessList:
                *.PUBLIC YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 0 :end
        :end
:end //of Asset

Asset:
        Name: Deployment Schedules :end
        Description: This is the long-term schedule for deployments. Everyone
wants to know the information contained in this asset. :end
        IsInstantiated: true :end
        HasDAC: true :end
        Secrecy: Secret :end
        DOSMotive: 5 :end
        AvailabilityPenalty: 500 :end
        AccessList:
                *.OperationsDepartment YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 80 :end
                AttackerMotive: 160 :end
        :end
        CostList:
                Access: *.CommunicationsDivision :end
                AccessMode: YYNN :end
                Cost: 80 :end
                AttackerMotive: 160 :end
        :end
        CostList:
                Access: *.AdministrativeDepartment :end
                AccessMode: YYNN :end
                Cost: 80 :end
                AttackerMotive: 160 :end
        :end
        CostList:
                Access: *.ShipsCompany :end
                AccessMode: YYNN :end
```

```
                Cost: 80 :end
                AttackerMotive: 160 :end
        :end
:end //of Asset

Asset:
        Name: CrewEvaluationReports :end
        Description: This asset contains all of the evaluation reports for the entire
command. :end
        IsInstantiated: true :end
        HasDAC: true :end
        Secrecy: Sensitive but unclassified :end
        DOSMotive: 0 :end
        AvailabilityPenalty: 500 :end
        AccessList:
                *.AdministrativeDepartment YYXX
        :end
        CostList:
                Access: *.Public :end
                AccessMode: YNNN :end
                Cost: 500 :end
                AttackerMotive: 50 :end
        :end
:end //of Asset

Asset:
        Name: SecretManuals :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: true :end
        Secrecy: Secret :end
        DOSMotive: 0 :end
        AvailabilityPenalty: 0 :end
        AccessList:
                LtDewitt YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 200 :end
                AttackerMotive: 0 :end
        :end
        CostList:
                Access: *.CommunicationsDivision :end
                AccessMode: YYNN :end
                Cost: 200 :end
```

```
            AttackerMotive: 90 :end
        :end
        CostList:
            Access: *.AdministrativeDepartment :end
            AccessMode: YYNN :end
            Cost: 200 :end
            AttackerMotive: 90 :end
        :end
        CostList:
            Access: *.ShipsCompany :end
            AccessMode: YYNN :end
            Cost: 200 :end
            AttackerMotive: 90 :end
        :end
:end //of Asset

Asset:
        Name: Readiness Reports :end
        Description: These are the reports that document the current operational
capability of this command. :end
        IsInstantiated: true :end
        HasDAC: false :end
        Secrecy: Confidential :end
        DOSMotive: 0 :end
        AvailabilityPenalty: 0 :end
        AccessList:
            *.OperationsDepartment YYXX
        :end
        CostList:
            Access: *.PUBLIC :end
            AccessMode: YYNN :end
            Cost: 0 :end
            AttackerMotive: 100 :end
        :end
        CostList:
            Access: *.CommunicationsDivision :end
            AccessMode: YYNN :end
            Cost: 250 :end
            AttackerMotive: 100 :end
        :end
        CostList:
            Access: *.AdministrativeDepartment :end
            AccessMode: YYNN :end
            Cost: 250 :end
            AttackerMotive: 100 :end
        :end
```

```
        CostList:
                Access: *.ShipsCompany :end
                AccessMode: YYNN :end
                Cost: 250 :end
                AttackerMotive: 100 :end
        :end
:end //of Asset

Asset:
        Name: Woodward's Stuff :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
        CreateWhilePaused: true :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                LTjgWoodward YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

Asset:
        Name: Packard's Stuff :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
        CreateWhilePaused: true :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                PO3Packard YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
```

```
:end //of Asset

Asset:
        Name: Dell's Stuff :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
        CreateWhilePaused: true :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                PO1Dell YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

Asset:
        Name: Gates' Stuff :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
        CreateWhilePaused: true :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                MCPOGates YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

Asset:
        Name: Torvalds' Stuff :end
        Description:  :end
        IsInstantiated: true :end
```

```
        HasDAC: false :end
        CreateWhilePaused: true :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                PO3Torvalds YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

Asset:
        Name: DeWitt's Stuff :end
        Description:  :end
        IsInstantiated: true :end
        HasDAC: false :end
        CreateWhilePaused: true :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                LtDewitt YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

Asset:
        Name: Hewlett's Stuff :end
        Description:  :end
        IsInstantiated: false :end
        HasDAC: false :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                ChiefHewlett YYXX
```

```
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

Asset:
        Name: Jones' Stuff :end
        Description:  :end
        IsInstantiated: false :end
        HasDAC: false :end
        Secrecy: Unclassified :end
        DOSMotive: 2 :end
        AvailabilityPenalty: 100 :end
        AccessList:
                SeamanJones YYXX
        :end
        CostList:
                Access: *.PUBLIC :end
                AccessMode: YYNN :end
                Cost: 0 :end
                AttackerMotive: 10 :end
        :end
:end //of Asset

AssetGoal:
        Name: Hewlett's Stuff :end
        Description: Chief Hewlett needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: Hewlett's Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 1000 :end
:end //of AssetGoal

AssetGoal:
        Name: Jones' Stuff :end
        Description: Seaman Jones needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: Jones' Stuff :end
```

```
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 1000 :end
:end //of AssetGoal

AssetGoal:
        Name: Dewitt's Stuff :end
        Description: DeWitt needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: DeWitt's Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 100 :end
:end //of AssetGoal

AssetGoal:
        Name: Torvald's Stuff :end
        Description: Torvalds needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: Torvalds' Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 100 :end
:end //of AssetGoal

AssetGoal:
        Name: Gates' Stuff :end
        Description: Gates needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: Gates' Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 100 :end
:end //of AssetGoal

AssetGoal:
        Name: Dell's Stuff :end
        Description: Dell needs access to his stuff :end
        Shared: false :end
```

```
        Asset:
                Name: Dell's Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 100 :end
:end //of AssetGoal

AssetGoal:
        Name: Packard's Stuff :end
        Description: Packard needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: Packard's Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 100 :end
:end //of AssetGoal

AssetGoal:
        Name: Woodward's Stuff :end
        Description: Woodward needs access to his stuff :end
        Shared: false :end
        Asset:
                Name: Woodward's Stuff :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 100 :end
:end //of AssetGoal

AssetGoal:
        Name: InternetAccess :end
        Description: Internet Access :end
        Shared: false :end
        Asset:
                Name: WebResources :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 5000 :end
:end //of AssetGoal

AssetGoal:
        Name: SecretAccess :end
```

```
        Description: Access to Secret Material :end
        Shared: false :end
        UseAssignedComputers: true :end
        Asset:
                Name: SecretManuals :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 800 :end
:end //of AssetGoal

AssetGoal:
        Name: ReadinessReportAccess :end
        Description: Access to the readiness reports :end
        Shared: false :end
        UseAssignedComputers: true :end
        Asset:
                Name: Readiness Reports :end
                filtered: false :end
                AccessMode: YYXX :end
        :end
        AvailabilityCostPenalty: 2000 :end
:end //of AssetGoal

AssetGoal:
        Name: DeploymentScheduleAccess :end
        Description: Access to the Deployment Schedule :end
        Shared: false :end
        UseAssignedComputers: true :end
        Asset:
                Name: Deployment Schedules :end
                filtered: false :end
                AccessMode: YXXX :end
        :end
        AvailabilityCostPenalty: 2000 :end
:end //of AssetGoal

AssetGoal:
        Name: Eval Report Access :end
        Description: Access to the Crew Evaluation Reports :end
        Shared: false :end
        Asset:
                Name: CrewEvaluationReports :end
                filtered: false :end
                AccessMode: YYXX :end
        :end
```

```
        AvailabilityCostPenalty: 1000 :end
:end //of AssetGoal

User:
        Name: LTjgWoodward :end
        Dept:  CommsDivision :end
        SecrecyClearance:  Secret :end
        DACGroups:
                PUBLIC :end
                CommunicationsDivision :end
                ShipsCompany :end
        :end
        DefaultDAC:  :end
        AssetGoal:
                AssetGoalName: InternetAccess :end
                TargetUsage: 5 :end
                Happiness: 20 :end
                Productivity: 20 :end
        :end
        AssetGoal:
                AssetGoalName: Woodward's Stuff :end
                TargetUsage: 5 :end
                Happiness: 25 :end
                Productivity: 0 :end
        :end
        Trustworthiness:  95 :end
        InitialTraining: 70 :end
        Happiness: 90 :end
        Productivity: 100 :end
        HISupportSkill: 70 :end
        PosIndex: 3 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: The Communications and ADP Officer :end
:end //of User

User:
        Name: PO3Packard :end
        Dept:  CommsDivision :end
        SecrecyClearance:  Secret :end
        DACGroups:
                PUBLIC :end
                CommunicationsDivision :end
                ShipsCompany :end
        :end
        DefaultDAC:  :end
```

```
        AssetGoal:
                AssetGoalName: InternetAccess :end
                TargetUsage: 5 :end
                Happiness: 25 :end
                Productivity: 25 :end
        :end
        AssetGoal:
                AssetGoalName: Packard's Stuff :end
                TargetUsage: 5 :end
                Happiness: 25 :end
                Productivity: 0 :end
        :end
        Trustworthiness:  70 :end
        InitialTraining: 70 :end
        Happiness: 70 :end
        Productivity: 100 :end
        HISupportSkill: 60 :end
        PosIndex: 5 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: Works in the Comms Office :end
:end //of User

User:
        Name: PO1Dell :end
        Dept:  operations :end
        SecrecyClearance:  Secret :end
        DACGroups:
                PUBLIC :end
                OperationsDepartment :end
                ShipsCompany :end
        :end
        DefaultDAC:  :end
        AssetGoal:
                AssetGoalName: InternetAccess :end
                TargetUsage: 5 :end
                Happiness: 50 :end
                Productivity: 50 :end
        :end
        AssetGoal:
                AssetGoalName: Dell's Stuff :end
                TargetUsage: 5 :end
                Happiness: 25 :end
                Productivity: 25 :end
        :end
        AssetGoal:
```

```
                AssetGoalName: ReadinessReportAccess :end
                TargetUsage: 5 :end
                Happiness: 5 :end
                Productivity: 0 :end
        :end
        Trustworthiness:  40 :end
        InitialTraining: 90 :end
        Happiness: 70 :end
        Productivity: 100 :end
        HISupportSkill: 90 :end
        PosIndex: 8 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: Works in the operations Office :end
:end //of User

User:
        Name: MCPOGates :end
        Dept:  Ship'sCompany :end
        SecrecyClearance:  Confidential :end
        DACGroups:
                PUBLIC :end
                ShipsCompany :end
        :end
        DefaultDAC:  :end
        AssetGoal:
                AssetGoalName: InternetAccess :end
                TargetUsage: 10 :end
                Happiness: 70 :end
                Productivity: 50 :end
        :end
        AssetGoal:
                AssetGoalName: Gates' Stuff :end
                TargetUsage: 5 :end
                Happiness: 25 :end
                Productivity: 25 :end
        :end
        Trustworthiness:  75 :end
        InitialTraining: 90 :end
        Happiness: 75 :end
        Productivity: 100 :end
        HISupportSkill: 95 :end
        PosIndex: 9 :end
        Cost: 0 :end
        Gender: male :end
```

UserDescription: Gates has reached the pinnacle of his profession and is riding the wave of his success. :end
:end //of User

User:
Name: PO3Torvalds :end
Dept: Ship'sCompany :end
SecrecyClearance: Sensitive but unclassified :end
DACGroups:
PUBLIC :end
ShipsCompany :end
:end
DefaultDAC: :end
AssetGoal:
AssetGoalName: InternetAccess :end
TargetUsage: 5 :end
Happiness: 55 :end
Productivity: 55 :end
:end
AssetGoal:
AssetGoalName: Torvald's Stuff :end
TargetUsage: 5 :end
Happiness: 25 :end
Productivity: 25 :end
:end
Trustworthiness: 90 :end
InitialTraining: 90 :end
Happiness: 99 :end
Productivity: 100 :end
HISupportSkill: 95 :end
PosIndex: 10 :end
Cost: 0 :end
Gender: male :end
UserDescription: An up and coming performer in the ship's company :end
:end //of User

User:
Name: LtDewitt :end
Dept: operations :end
SecrecyClearance: Secret :end
DACGroups:
PUBLIC :end
OperationsDepartment :end
ShipsCompany :end
:end
DefaultDAC: :end

```
        AssetGoal:
                AssetGoalName: SecretAccess :end
                TargetUsage: 5 :end
                Happiness: 15 :end
                Productivity: 15 :end
        :end
        AssetGoal:
                AssetGoalName: Dewitt's Stuff :end
                TargetUsage: 5 :end
                Happiness: 25 :end
                Productivity: 25 :end
        :end
        Trustworthiness:  95 :end
        InitialTraining: 60 :end
        Happiness: 80 :end
        Productivity: 100 :end
        HISupportSkill: 75 :end
        PosIndex: 6 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: The Operations Officer :end
:end //of User

User:
        Name: ChiefHewlett :end
        Dept:  admin :end
        SecrecyClearance:  Secret :end
        DACGroups:
                PUBLIC :end
                AdministrativeDepartment :end
                ShipsCompany :end
        :end
        DefaultDAC:  :end
        AssetGoal:
                AssetGoalName: InternetAccess :end
                TargetUsage: 0 :end
                Happiness: 55 :end
                Productivity: 55 :end
        :end
        AssetGoal:
                AssetGoalName: Hewlett's Stuff :end
                TargetUsage: 0 :end
                Happiness: 20 :end
                Productivity: 20 :end
        :end
        Trustworthiness:  80 :end
```

```
        InitialTraining: 85 :end
        Happiness: 90 :end
        Productivity: 100 :end
        HISupportSkill: 95 :end
        PosIndex: 1 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: The Admin Officer :end
:end //of User

User:
        Name: SeamanJones :end
        Dept:  admin :end
        SecrecyClearance:  Confidential :end
        DACGroups:
                PUBLIC :end
                AdministrativeDepartment :end
                ShipsCompany :end
        :end
        DefaultDAC:  :end
        AssetGoal:
                AssetGoalName: InternetAccess :end
                TargetUsage: 0 :end
                Happiness: 55 :end
                Productivity: 55 :end
        :end
        AssetGoal:
                AssetGoalName: Jones' Stuff :end
                TargetUsage: 0 :end
                Happiness: 15 :end
                Productivity: 20 :end
        :end
        Trustworthiness:  55 :end
        InitialTraining: 60 :end
        Happiness: 80 :end
        Productivity: 100 :end
        HISupportSkill: 40 :end
        PosIndex: 2 :end
        Cost: 0 :end
        Gender: male :end
        UserDescription: Works in the Admin Department :end
:end //of User

User: //SupportStaff
        Name: Seaman Dowdy :end
        Dept:  Security :end
```

HWSupportSkill: 80 :end
SWSupportSkill: 80 :end
HISupportSkill: 80 :end
DaysTillAvailable: 0 :end
Trustworthiness: 80 :end
InitialTraining: 80 :end
Happiness: 80 :end
Productivity: 80 :end
Skill: 80 :end
PosIndex: 0 :end
Cost: 2500 :end
Gender: male :end
UserDescription: Dowdy is on duty. Do you want him to work in your zones? :end
:end //of SupportStaff

User: //SupportStaff
Name: EnsignPulver :end
Dept: Security :end
HWSupportSkill: 20 :end
SWSupportSkill: 20 :end
HISupportSkill: 50 :end
DaysTillAvailable: 0 :end
Trustworthiness: 30 :end
InitialTraining: 30 :end
Happiness: 99 :end
Productivity: 20 :end
Skill: 20 :end
PosIndex: 0 :end
Cost: 3000 :end
Gender: male :end
UserDescription: Ensign Pulver is the Assistant Duty Officer. Hire him if you want him to provide security in this zone. :end
:end //of SupportStaff

User: //SupportStaff
Name: LtRoberts :end
Dept: Security :end
HWSupportSkill: 50 :end
SWSupportSkill: 50 :end
HISupportSkill: 99 :end
Trustworthiness: 90 :end
InitialTraining: 90 :end
Happiness: 80 :end
Productivity: 80 :end
Skill: 99 :end

PosIndex: 0 :end
Cost: 4000 :end
Gender: male :end
UserDescription: LT Roberts is the Duty Officer. As such, he is responsible for enforcing the Organization's Security Policy. :end
:end //of SupportStaff

User: //SupportStaff
Name: PO1Farragut :end
Dept: Tech :end
HWSupportSkill: 95 :end
SWSupportSkill: 95 :end
HISupportSkill: 45 :end
DaysTillAvailable: 0 :end
Trustworthiness: 95 :end
InitialTraining: 50 :end
Happiness: 85 :end
Productivity: 80 :end
Skill: 90 :end
PosIndex: 4 :end
Cost: 3000 :end
Gender: male :end
UserDescription: Petty Officer Farragut is a superstar troubleshooter and a top notch system administrator. :end
:end //of SupportStaff

User: //SupportStaff
Name: PO1Spruance :end
Dept: Tech :end
HWSupportSkill: 95 :end
SWSupportSkill: 95 :end
HISupportSkill: 80 :end
DaysTillAvailable: 0 :end
Trustworthiness: 95 :end
InitialTraining: 95 :end
Happiness: 90 :end
Productivity: 90 :end
Skill: 90 :end
PosIndex: 0 :end
Cost: 2000 :end
Gender: male :end
UserDescription: PO1 Spruance is known as the Quiet Warrior to his shipmates. :end
:end //of SupportStaff

User: //SupportStaff

Name: PO2Bulkeley :end
Dept: Tech :end
HWSupportSkill: 100 :end
SWSupportSkill: 100 :end
HISupportSkill: 10 :end
DaysTillAvailable: 0 :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 0 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Petty Officer Bulkeley would rather be on a PT boat. :end
:end //of SupportStaff

User: //SupportStaff
Name: PO2 Nimitz :end
Dept: Tech :end
HWSupportSkill: 50 :end
SWSupportSkill: 50 :end
HISupportSkill: 50 :end
DaysTillAvailable: 0 :end
Trustworthiness: 50 :end
InitialTraining: 50 :end
Happiness: 50 :end
Productivity: 50 :end
Skill: 50 :end
PosIndex: 0 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Nimitz wishes he was in Hawaii. :end
:end //of SupportStaff

User: //SupportStaff
Name: PO3 Halsey :end
Dept: Tech :end
HWSupportSkill: 50 :end
SWSupportSkill: 50 :end
HISupportSkill: 50 :end
DaysTillAvailable: 0 :end
Trustworthiness: 50 :end
InitialTraining: 50 :end
Happiness: 50 :end
Productivity: 50 :end

Skill: 100 :end
Posindex: 0 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Although bold and decisive, Halsey doesn't necessarily make the best decisions. :end
:end //of SupportStaff

User: //SupportStaff
Name: SeamanDewey :end
Dept: Tech :end
HWSupportSkill: 80 :end
SWSupportSkill: 80 :end
HISupportSkill: 40 :end
DaysTillAvailable: 0 :end
Trustworthiness: 40 :end
InitialTraining: 40 :end
Happiness: 40 :end
Productivity: 40 :end
Skill: 40 :end
Posindex: 0 :end
Cost: 2000 :end
Gender: male :end
UserDescription: :end
:end //of SupportStaff

User: //SupportStaff
Name: SeamanNelson :end
Dept: Tech :end
HWSupportSkill: 100 :end
SWSupportSkill: 100 :end
HISupportSkill: 100 :end
DaysTillAvailable: 0 :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
Posindex: 0 :end
Cost: 3000 :end
Gender: male :end
UserDescription: Seaman Nelson made a name for himself at Trafalgar :end
:end //of SupportStaff

Workspace:

```
        PosIndex: 0 :end
        Type: Server :end
:end

Workspace:
        PosIndex: 1 :end
:end

Workspace:
        PosIndex: 2 :end
:end

Workspace:
        PosIndex: 3 :end
:end

Workspace:
        PosIndex: 4 :end
        Type: Server :end
:end

Workspace:
        PosIndex: 5 :end
:end

Workspace:
        PosIndex: 6 :end
:end

Workspace:
        PosIndex: 7 :end
        Type: Server :end
:end

Workspace:
        PosIndex: 8 :end
:end

Workspace:
        PosIndex: 9 :end
:end

Workspace:
        PosIndex: 10 :end
:end
```

Component: //start of the physical component section.
Name: SIPRNET Gateway Router :end
IsTemplate: false :end
Description: :end
AssetProtection: false :end
HW: Bit Flipper Switch :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: :end
PosIndex: 0 :end
UninterruptiblePower: false :end
//NetworkConnections:
Network:
Name: SiprLan :end
:end //end of NetworkConnections:
Network:
Name: SIPRNET :end
:end //end of NetworkConnections:
ComponentProceduralSettings:
HoldsUserAsset: false :end
MaxSecrecyLabel: Secret :end
MinSecrecyLabel: Unclassified :end

ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: medium :end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Regular :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: Niprlan2dmz :end
IsTemplate: false :end
Description: :end
AssetProtection: false :end
HW: CP Router :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end

EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: :end
PosIndex: 4 :end
UninterruptiblePower: false :end
//NetworkConnections:
Network:
Name: NiprLan :end
:end //end of NetworkConnections:
Network:
Name: UnclassDMZ :end
:end //end of NetworkConnections:
:end //of physical component Section

Component: //start of the physical component section.
Name: INTERNET Gateway Router :end
IsTemplate: false :end
Description: :end
AssetProtection: false :end
HW: CP Router :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end

BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: :end
PosIndex: 4 :end
UninterruptiblePower: false :end
//NetworkConnections:
Network:
Name: Internet :end
:end //end of NetworkConnections:
Network:
Name: UnclassDMZ :end
:end //end of NetworkConnections:
ComponentProceduralSettings:
HoldsUserAsset: false :end
MaxSecrecyLabel: Sensitive but unclassified :end
MinSecrecyLabel: Unclassified :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: medium :end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: InternetRouters :end
IsTemplate: false :end
Description: :end
AssetProtection: false :end
HW: CP Router :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end

Availability: 99 :end
Static: true :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: :end
PosIndex: 7 :end
UninterruptiblePower: false :end
//NetworkConnections:
Network:
	Name: Internet :end
:end	//end of NetworkConnections:
Network:
	Name: OffsiteNetworks :end
:end	//end of NetworkConnections:
ComponentProceduralSettings:
	HoldsUserAsset: false :end
	MaxSecrecyLabel: Sensitive but unclassified :end
	MinSecrecyLabel: Unclassified :end
	ProtectWithACL: true :end
	WriteDownPasswords: false :end
	LockorLogoff: true :end
	PasswordLength: medium :end
	PasswordCharacterSet: complex :end
	PasswordChangeFrequency: six :end
	NoEmailAttachmentExecute: true :end
	NoExternalSoftware: true :end
	NoUseOfModems: true :end

NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: World Wide Web :end
IsTemplate: false :end
Description: :end
AssetProtection: true :end
HW: Blato Server :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 100 :end
Static: true :end
OS: Populos V9 Server :end
Software: Populos Web Slave :end
Software: Internet Contemplator :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: true :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: true :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: true :end
BrowserSettings: Strict :end
EmailSettings: Strict :end
UpdatePatches: AsReleased :end
ManagedAntivirus: true :end
User: :end
PosIndex: 7 :end

```
        Assets: WebResources :end
        AccessListLocal: *.Public :end
        AccessListRemote: *.Public :end
        UninterruptiblePower: true :end
        CM: Strong :end
        //NetworkConnections:
        Network:
                Name: OffsiteNetworks :end
        :end    //end of NetworkConnections:
        ComponentProceduralSettings:
                HoldsUserAsset: false :end
                MaxSecrecyLabel: Sensitive but unclassified :end
                MinSecrecyLabel: Unclassified :end
                ProtectWithACL: true :end
                WriteDownPasswords: false :end
                LockorLogoff: true :end
                PasswordLength: medium :end
                PasswordCharacterSet: complex :end
                PasswordChangeFrequency: six :end
                NoEmailAttachmentExecute: true :end
                NoExternalSoftware: true :end
                NoUseOfModems: true :end
                NoWebMail: true :end
                NoMediaLeaveZone: true :end
                UpdateAntiVirus: Automatic :end
                ApplyPatches: false :end
                LeaveMachinesOn: true :end
                NoPhysicalModifications: false :end
                UserBackup: true :end
        :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
        Name: OpsNiprnet1 :end
        IsTemplate: false :end
        Description:  :end
        AssetProtection: true :end
        HW: Blato Desktop Select :end
        Cost: 0 :end
        Resale: 0 :end
        Maintenance: 0 :end
        Availability: 99 :end
        Static: false :end
        OS: Populos V9 Desktop :end
        Software: Viewpoint :end
        Software: Internet Contemplator :end
```

Software: Palm Reader :end
Software: Thin Man :end
Software: Populos Client :end
Software: Populos SPF 30 :end
Software: Placebo :end
Software: Zone Out :end
Software: Extortos :end
Software: URL2U :end
Software: Euphoria :end
Software: Populos VPN Client :end
Software: Bit Flip Client :end
Software: MatTracker :end
Software: Word Triangle :end
Software: Spread Triangle :end
Software: WordSmyth :end
Software: Cell Life :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: false :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: true :end
BlockLocalStorage: false :end
BrowserSettings: Normal :end
EmailSettings: Normal :end
UpdatePatches: AsReleased :end
ManagedAntivirus: true :end
User: PO1Dell :end
PosIndex: 8 :end
Assets: Dell's Stuff :end
UninterruptiblePower: true :end
CM: Strong :end
//NetworkConnections:
Network:
        Name: NiprLan :end
:end   //end of NetworkConnections:
ComponentProceduralSettings:

HoldsUserAsset: false :end
MaxSecrecyLabel: Sensitive but unclassified :end
MinSecrecyLabel: Unclassified :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: medium :end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: Commniprnet1 :end
IsTemplate: false :end
Description: :end
AssetProtection: true :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
Software: Viewpoint :end
Software: Internet Contemplator :end
Software: Palm Reader :end
Software: Thin Man :end
Software: Populos Client :end
Software: Populos SPF 30 :end
Software: Placebo :end
Software: Zone Out :end
Software: Extortos :end
Software: URL2U :end
Software: Euphoria :end
Software: Populos VPN Client :end

Software: Bit Flip Client :end
Software: MatTracker :end
Software: Word Triangle :end
Software: Spread Triangle :end
Software: WordSmyth :end
Software: Cell Life :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: false :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: true :end
BlockLocalStorage: false :end
BrowserSettings: Normal :end
EmailSettings: Normal :end
UpdatePatches: AsReleased :end
ManagedAntivirus: true :end
User: LTjgWoodward :end
PosIndex: 3 :end
Assets: Woodward's Stuff :end
UninterruptiblePower: true :end
CM: Strong :end
//NetworkConnections:
Network:
	Name: NiprLan :end
:end	//end of NetworkConnections:
ComponentProceduralSettings:
	HoldsUserAsset: false :end
	MaxSecrecyLabel: Sensitive but unclassified :end
	MinSecrecyLabel: Unclassified :end
	ProtectWithACL: true :end
	WriteDownPasswords: false :end
	LockorLogoff: true :end
	PasswordLength: medium :end
	PasswordCharacterSet: complex :end
	PasswordChangeFrequency: six :end
	NoEmailAttachmentExecute: true :end

NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: Commniprnet2 :end
IsTemplate: false :end
Description: :end
AssetProtection: true :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
Software: Viewpoint :end
Software: Internet Contemplator :end
Software: Palm Reader :end
Software: Thin Man :end
Software: Populos Client :end
Software: Populos SPF 30 :end
Software: Placebo :end
Software: Zone Out :end
Software: Extortos :end
Software: URL2U :end
Software: Euphoria :end
Software: Populos VPN Client :end
Software: Bit Flip Client :end
Software: MatTracker :end
Software: Word Triangle :end
Software: Spread Triangle :end
Software: WordSmyth :end
Software: Cell Life :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end

UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: false :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: true :end
BlockLocalStorage: false :end
BrowserSettings: Normal :end
EmailSettings: Normal :end
UpdatePatches: AsReleased :end
ManagedAntivirus: true :end
User: PO3Packard :end
PosIndex: 5 :end
Assets: Packard's Stuff :end
UninterruptiblePower: true :end
CM: Strong :end
//NetworkConnections:
Network:
Name: NiprLan :end
:end //end of NetworkConnections:
ComponentProceduralSettings:
HoldsUserAsset: false :end
MaxSecrecyLabel: Sensitive but unclassified :end
MinSecrecyLabel: Unclassified :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: medium :end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
:end //of ComponentProceduralSettings

:end //of physical component Section

Component: //start of the physical component section.
Name: OpenComputer1 :end
IsTemplate: false :end
Description: :end
AssetProtection: true :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
Software: Viewpoint :end
Software: Internet Contemplator :end
Software: Palm Reader :end
Software: Thin Man :end
Software: Populos Client :end
Software: Populos SPF 30 :end
Software: Placebo :end
Software: Zone Out :end
Software: Extortos :end
Software: URL2U :end
Software: Euphoria :end
Software: Populos VPN Client :end
Software: Bit Flip Client :end
Software: MatTracker :end
Software: Word Triangle :end
Software: Spread Triangle :end
Software: WordSmyth :end
Software: Cell Life :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: false :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end

EnforcePasswordPolicy: true :end
BlockLocalStorage: false :end
BrowserSettings: Normal :end
EmailSettings: Normal :end
UpdatePatches: AsReleased :end
ManagedAntivirus: true :end
User: MCPOGates :end
PosIndex: 9 :end
Assets: Gates' Stuff :end
UninterruptiblePower: true :end
CM: Strong :end
//NetworkConnections:
Network:
Name: NiprLan :end
:end //end of NetworkConnections:
ComponentProceduralSettings:
HoldsUserAsset: false :end
MaxSecrecyLabel: Sensitive but unclassified :end
MinSecrecyLabel: Unclassified :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: medium :end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: Automatic :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: OpenComputer2 :end
IsTemplate: false :end
Description: :end
AssetProtection: true :end
HW: Blato Desktop Select :end
Cost: 0 :end
Resale: 0 :end

Maintenance: 0 :end
Availability: 99 :end
Static: false :end
OS: Populos V9 Desktop :end
Software: Viewpoint :end
Software: Internet Contemplator :end
Software: Palm Reader :end
Software: Thin Man :end
Software: Populos Client :end
Software: Populos SPF 30 :end
Software: Placebo :end
Software: Zone Out :end
Software: Extortos :end
Software: URL2U :end
Software: Euphoria :end
Software: Populos VPN Client :end
Software: Bit Flip Client :end
Software: MatTracker :end
Software: Word Triangle :end
Software: Spread Triangle :end
Software: WordSmyth :end
Software: Cell Life :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: false :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: true :end
BlockLocalStorage: false :end
BrowserSettings: Normal :end
EmailSettings: Normal :end
UpdatePatches: AsReleased :end
ManagedAntivirus: true :end
User: PO3Torvalds :end
PosIndex: 10 :end
Assets: Torvalds' Stuff :end
UninterruptiblePower: true :end

```
        CM: Strong :end
        //NetworkConnections:
        Network:
                Name: NiprLan :end
        :end    //end of NetworkConnections:
        ComponentProceduralSettings:
                HoldsUserAsset: false :end
                MaxSecrecyLabel: Sensitive but unclassified :end
                MinSecrecyLabel: Unclassified :end
                ProtectWithACL: true :end
                WriteDownPasswords: false :end
                LockorLogoff: true :end
                PasswordLength: medium :end
                PasswordCharacterSet: complex :end
                PasswordChangeFrequency: six :end
                NoEmailAttachmentExecute: true :end
                NoExternalSoftware: true :end
                NoUseOfModems: true :end
                NoWebMail: true :end
                NoMediaLeaveZone: true :end
                UpdateAntiVirus: Automatic :end
                ApplyPatches: false :end
                LeaveMachinesOn: true :end
                NoPhysicalModifications: false :end
                UserBackup: true :end
        :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
        Name: SecretServer :end
        IsTemplate: false :end
        Description: This is the Ship's Secret Level Intranet Server :end
        AssetProtection: false :end
        HW: Blato Server :end
        Cost: 0 :end
        Resale: 0 :end
        Maintenance: 0 :end
        Availability: 100 :end
        Static: false :end
        OS: Trusted Populos Server :end
        RemoteAuthentication: false :end
        AcceptPKICerts: false :end
        UseOneTimePasswordToken: false :end
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
        UseClientPKICerts: false :end
```

VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: true :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Strict :end
EmailSettings: Strict :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: :end
PosIndex: 0 :end
Assets: Readiness Reports :end
Assets: Deployment Schedules :end
AccessListLocal: LtDewitt :end
AccessListLocal: LTjgWoodward :end
AccessListLocal: PO1Dell :end
AccessListRemote: LtDewitt :end
UninterruptiblePower: true :end
//NetworkConnections:
Network:
	Name: SiprLan :end
:end	//end of NetworkConnections:
ComponentProceduralSettings:
	HoldsUserAsset: false :end
	MaxSecrecyLabel: Secret :end
	MinSecrecyLabel: Unclassified :end
	ProtectWithACL: false :end
	WriteDownPasswords: false :end
	LockorLogoff: false :end
	PasswordLength: none :end
	PasswordCharacterSet: any :end
	PasswordChangeFrequency: never :end
	NoEmailAttachmentExecute: false :end
	NoExternalSoftware: false :end
	NoUseOfModems: false :end
	NoWebMail: false :end
	NoMediaLeaveZone: false :end
	ApplyPatches: false :end
	LeaveMachinesOn: false :end
	NoPhysicalModifications: false :end
	UserBackup: false :end

:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
Name: UnclassServer :end
IsTemplate: false :end
Description: This is the Ship's web server. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 0 :end
Resale: 0 :end
Maintenance: 0 :end
Availability: 100 :end
Static: false :end
OS: Trusted Populos Server :end
Software: Populos SSH :end
Software: Populos FTP :end
Software: Populos Telnet :end
Software: Populos Web Slave :end
Software: Populus Letter Pusher :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: false :end
EnforcePasswordPolicy: false :end
BlockLocalStorage: false :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: None :end
ManagedAntivirus: false :end
User: :end
PosIndex: 4 :end
Assets: CrewEvaluationReports :end
AccessListLocal: LTjgWoodward :end
AccessListLocal: PO3Packard :end
AccessListRemote: *.CommunicationsDivision :end

```
        AccessListRemote: *.OperationsDepartment :end
        UninterruptiblePower: false :end
        //NetworkConnections:
        Network:
                Name: UnclassDMZ :end
        :end    //end of NetworkConnections:
        ComponentProceduralSettings:
                HoldsUserAsset: false :end
                MaxSecrecyLabel: Secret :end
                MinSecrecyLabel: Unclassified :end
                ProtectWithACL: false :end
                WriteDownPasswords: false :end
                LockorLogoff: false :end
                PasswordLength: none :end
                PasswordCharacterSet: any :end
                PasswordChangeFrequency: never :end
                NoEmailAttachmentExecute: false :end
                NoExternalSoftware: false :end
                NoUseOfModems: false :end
                NoWebMail: false :end
                NoMediaLeaveZone: false :end
                ApplyPatches: false :end
                LeaveMachinesOn: false :end
                NoPhysicalModifications: false :end
                UserBackup: false :end
        :end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the physical component section.
        Name: OpsSiprnet :end
        IsTemplate: false :end
        Description: This computer is assigned to the Operations Officer :end
        AssetProtection: true :end
        HW: Blato Desktop Select :end
        Cost: 0 :end
        Resale: 0 :end
        Maintenance: 0 :end
        Availability: 99 :end
        Static: false :end
        OS: Populos V9 Desktop :end
        Software: Internet Contemplator :end
        RemoteAuthentication: false :end
        AcceptPKICerts: false :end
        UseOneTimePasswordToken: false :end
        UseBiometrics: false :end
        UseTokenPKICerts: false :end
```

UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: true :end
StripEmailAttachments: true :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
UserRunsPrivileged: false :end
BlockRemovableMedia: true :end
EnforcePasswordPolicy: true :end
BlockLocalStorage: false :end
BrowserSettings: Strict :end
EmailSettings: Strict :end
UpdatePatches: Regular :end
ManagedAntivirus: true :end
User: LtDewitt :end
PosIndex: 6 :end
Assets: SecretManuals :end
Assets: DeWitt's Stuff :end
AccessListLocal: LtDewitt :end
AccessListLocal: LTjgWoodward :end
AccessListLocal: PO3Packard :end
UninterruptiblePower: true :end
CM: Strong :end
//NetworkConnections:
Network:
	Name: SiprLan :end
:end	//end of NetworkConnections:
ComponentProceduralSettings:
	HoldsUserAsset: false :end
	MaxSecrecyLabel: Secret :end
	MinSecrecyLabel: Unclassified :end
	ProtectWithACL: true :end
	WriteDownPasswords: false :end
	LockorLogoff: true :end
	PasswordLength: medium :end
	PasswordCharacterSet: complex :end
	PasswordChangeFrequency: six :end
	NoEmailAttachmentExecute: true :end
	NoExternalSoftware: true :end
	NoUseOfModems: true :end
	NoWebMail: true :end
	NoMediaLeaveZone: true :end
	UpdateAntiVirus: Regular :end
	UpdateAntiVirus: Automatic :end
	ApplyPatches: false :end

LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: true :end
:end //of ComponentProceduralSettings
:end //of physical component Section

Component: //start of the catalog component section.
Name: Blato Desktop Select :end
IsTemplate: true :end
Description: Packed with applications, memory and disk :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 1700 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
Software: WordSmyth :end
Software: Cell Life :end
Software: Internet Contemplator :end
Software: Viewpoint :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: NORMAL :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Targo Worksaver :end
IsTemplate: true :end

Description: Full suite of productivity software, adequate memory and dis.
:end
AssetProtection: false :end
HW: Targo Worksaver :end
Cost: 1700 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
Software: WordSmyth :end
Software: Cell Life :end
Software: Viewpoint :end
Software: Internet Contemplator :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Trusted Targo Worksaver :end
IsTemplate: true :end
Description: Similar to the Targo Worksaver, but includes the Trusted
Populos OS. :end
AssetProtection: false :end
HW: Trusted Targo Worksaver :end
Cost: 2500 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Trusted Populos Desktop :end

Software: WordSmyth :end
Software: Cell Life :end
Software: Internet Contemplator :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: The Thin Man :end
IsTemplate: true :end
Description: A thin client intended to work with either Gossamer products or Populos Terminal Servers. :end
AssetProtection: false :end
HW: The Thin Man :end
Cost: 900 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos Embedded V5 :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end

SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Green Net Client :end
IsTemplate: true :end
Description: A thin client intended to work with Gossamer products. Intended use is to connect to multiple networks of different sensitivity levels :end
AssetProtection: false :end
HW: Green Net Client :end
Cost: 3000 :end
Resale: 1000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Desktop :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Lunitos AFOS :end

IsTemplate: true :end
Description: Sleek colorful desktop machine with adequate memory and disk :end
AssetProtection: false :end
HW: Lunitos AFOS :end
Cost: 2300 :end
Resale: 300 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Lunitos Desktop :end
Software: URL2U :end
Software: Euphoria :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Greenshade Client :end
IsTemplate: true :end
Description: High assurance client workstation having the Secure Shade Desktop O/S. :end
AssetProtection: false :end
HW: Blato Desktop Select :end
Cost: 4200 :end
Resale: 800 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Desktop :end
Software: Word Triangle :end

Software: Spread Triangle :end
Software: URL2U :end
Software: Euphoria :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Targo Server :end
IsTemplate: true :end
Description: Full featured server with the worlds most popular operating system. :end
AssetProtection: false :end
HW: Targo Server :end
Cost: 15000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end

SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Blato Server :end
IsTemplate: true :end
Description: Full featured server with the worlds most popular operating system. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 15000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Twist Off Server :end

IsTemplate: true :end
Description: Server class machine with the Jar Lid Server O/S :end
AssetProtection: false :end
HW: Twist Off Server :end
Cost: 10000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Twister Terminal Server :end
IsTemplate: true :end
Description: Terminal server capable of presenting Jar Lid applications to thin client workstations. :end
AssetProtection: false :end
HW: Twist Off Server :end
Cost: 10000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end

UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Green Shade Server :end
IsTemplate: true :end
Description: Server class machine with the Secure Shade Server high assurance operating system :end
AssetProtection: false :end
HW: Green Shade Server :end
Cost: 80000 :end
Resale: 20000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end

UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Mail Appliance :end
IsTemplate: true :end
Description: Simple Email Server. :end
AssetProtection: false :end
HW: Targo Server :end
Cost: 5000 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Populos Letter Pusher :end
IsTemplate: true :end
Description: Email Server that rules. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 20000 :end
Resale: 8000 :end
Maintenance: 100 :end
Availability: 99 :end

OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Web Appliance :end
IsTemplate: true :end
Description: Simple web server :end
AssetProtection: false :end
HW: Twist Off Server :end
Cost: 1500 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end

BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Populos Internet Slave :end
IsTemplate: true :end
Description: Web Server that rules the web. :end
AssetProtection: false :end
HW: Blato Server :end
Cost: 10000 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bit Flipper :end
IsTemplate: true :end
Description: High performance router :end
AssetProtection: false :end
HW: Bit Flipper :end

Cost: 150 :end
Resale: 60 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bit Flipper VPN :end
IsTemplate: true :end
Description: VPN Gateway -- another Bit Flipper product :end
AssetProtection: false :end
HW: Bit Flipper VPN :end
Cost: 200 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end

AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bent Line VPN :end
IsTemplate: true :end
Description: VPN Gateway Evaluated to EAL4+ :end
AssetProtection: false :end
HW: Bent Line VPN :end
Cost: 1500 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V8 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Green Shade VPN :end

IsTemplate: true :end
Description: VPN Gateway On a Green Shade Core :end
AssetProtection: false :end
HW: Green Shade VPN :end
Cost: 1500 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: GEOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Crack This! :end
IsTemplate: true :end
Description: Best Selling VPN Gateway :end
AssetProtection: false :end
HW: Crack This! :end
Cost: 1500 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end

UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Five Inches of Asbestos :end
IsTemplate: true :end
Description: Best selling firewall :end
AssetProtection: false :end
HW: Five Inches of Asbestos :end
Cost: 900 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end

:end //of catalog component Section

Component: //start of the catalog component section.
Name: Bit Flipper Border :end
IsTemplate: true :end
Description: Full featured firewall :end
AssetProtection: false :end
HW: Bit Flipper Border :end
Cost: 200 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Wire Stuff :end
IsTemplate: true :end
Description: High quality hub with high reliability :end
AssetProtection: false :end
HW: Wire Stuff :end
Cost: 150 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end

AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Component: //start of the catalog component section.
Name: Box with Wires :end
IsTemplate: true :end
Description: General purpose hub :end
AssetProtection: false :end
HW: Box with Wires :end
Cost: 90 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
AutomaticLockLogout: false :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end

BrowserSettings: LOOSE :end
EmailSettings: LOOSE :end
UpdatePatches: NONE :end
UpdateAntivirus: NONE :end
:end //of catalog component Section

Conditions:
Condition:
Tagname: deploymentscedsattacked :end
ConditionClass: AssetAttacked :end
ConditionText: Deployment Schedules :end
Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: evalreportsattacked :end
ConditionClass: AssetAttacked :end
ConditionText: CrewEvaluationReports :end
Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: secretmanualsattacked :end
ConditionClass: AssetAttacked :end
ConditionText: SecretManuals :end
Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: readinessreportsattacked :end
ConditionClass: AssetAttacked :end
ConditionText: Readiness Reports :end
Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: woodwardsstuffattacked :end
ConditionClass: AssetAttacked :end

```
            ConditionText: Woodward's Stuff :end
            Parameter: -1 :end
            Parameter: 0 :end
            Parameter: 2000 :end
:end //of Condition

    Condition:
            Tagname: packardsstuffattacked :end
            ConditionClass: AssetAttacked :end
            ConditionText: Packard's Stuff :end
            Parameter: -1 :end
            Parameter: 0 :end
            Parameter: 2000 :end
:end //of Condition

    Condition:
            Tagname: dellsstuffattacked :end
            ConditionClass: AssetAttacked :end
            ConditionText: Dell's Stuff :end
            Parameter: -1 :end
            Parameter: 0 :end
            Parameter: 2000 :end
:end //of Condition

    Condition:
            Tagname: gatesstuffattacked :end
            ConditionClass: AssetAttacked :end
            ConditionText: Gates' Stuff :end
            Parameter: -1 :end
            Parameter: 0 :end
            Parameter: 2000 :end
:end //of Condition

    Condition:
            Tagname: torvaldsstuffattacked :end
            ConditionClass: AssetAttacked :end
            ConditionText: Torvalds' Stuff :end
            Parameter: -1 :end
            Parameter: 0 :end
            Parameter: 2000 :end
:end //of Condition

    Condition:
            Tagname: dewittsstuffattacked :end
            ConditionClass: AssetAttacked :end
            ConditionText: DeWitt's Stuff :end
```

Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: hewlettstuffattacked :end
ConditionClass: AssetAttacked :end
ConditionText: Hewlett's Stuff :end
Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: jonesstuffattacked :end
ConditionClass: AssetAttacked :end
ConditionText: Jones' Stuff :end
Parameter: -1 :end
Parameter: 0 :end
Parameter: 2000 :end
:end //of Condition

Condition:
Tagname: SecretMantoNiprnet :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: SecretManuals :end
SecondConditionText: NiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: ReadinessReportNiprnet :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Readiness Reports :end
SecondConditionText: NiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: evalreportstosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: SiprLan :end

ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: jonestosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Jones' Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: hewletttosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Hewlett's Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: dewitttosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: DeWitt's Stuff :end
SecondConditionText: NiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: torvaldtosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Torvalds' Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: gatestosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Gates' Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end

Parameter: 0 :end
:end //of Condition

Condition:
Tagname: delltosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Dell's Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: packardtosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Packard's Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: woodwardtosipr :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Woodward's Stuff :end
SecondConditionText: SiprLan :end
ThirdConditionText: none :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: endphase1 :end
ConditionClass: PhaseCompleted :end
ConditionText: 21 :end
:end //of Condition

Condition:
Tagname: endphase2 :end
ConditionClass: PhaseCompleted :end
ConditionText: 22 :end
:end //of Condition

Condition:
Tagname: endphase3 :end
ConditionClass: PhaseCompleted :end
ConditionText: 23 :end

:end //of Condition

Condition:
Tagname: endphase4 :end
ConditionClass: PhaseCompleted :end
ConditionText: 24 :end
:end //of Condition

Condition:
Tagname: gameonscreen :end
ConditionClass: GameOnScreen :end
Parameter: 1 :end
:end //of Condition

Condition:
Tagname: unclass2dmzemail :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: NiprLan :end
ThirdConditionText: EMAIL SERVER :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: niprlantodmzweb :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: NiprLan :end
ThirdConditionText: WEB SERVER :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: dmz2internetweb :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: Internet :end
ThirdConditionText: WEB SERVER :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: dmz2internettelnet :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: Internet :end

ThirdConditionText: TELNET :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: dmztointernetemail :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: Internet :end
ThirdConditionText: EMAIL SERVER :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: siprserverav :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: UpdateAntivirus:Regular :end
:end //of Condition

Condition:
Tagname: siprserverav2 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: UpdateAntivirus:Automatic :end
:end //of Condition

Condition:
Tagname: niprserverav :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: UpdateAntivirus:Automatic :end
:end //of Condition

Condition:
Tagname: niprserverav2 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: UpdateAntivirus:Regular :end
:end //of Condition

Condition:
Tagname: niprserverbackup :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: OffsiteBackup: :end

:end //of Condition

Condition:
Tagname: siprserverbackup :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: OffsiteBackup: :end
:end //of Condition

Condition:
Tagname: npatch :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: UpdatePatches:Regular :end
:end //of Condition

Condition:
Tagname: npatch2 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: UpdatePatches:Automatic :end
:end //of Condition

Condition:
Tagname: npatch3 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: UpdatePatches:AsReleased :end
:end //of Condition

Condition:
Tagname: ncm1 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: CM:Weak :end
:end //of Condition

Condition:
Tagname: ncm2 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: CM:Moderate :end
:end //of Condition

Condition:
Tagname: ncm3 :end

ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: CM:Strong :end
:end //of Condition

Condition:
Tagname: spatch :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: UpdatePatches:Regular :end
:end //of Condition

Condition:
Tagname: spatch2 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: UpdatePatches:Automatic :end
:end //of Condition

Condition:
Tagname: spatch3 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: UpdatePatches:AsReleased :end
:end //of Condition

Condition:
Tagname: scm1 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: CM:Weak :end
:end //of Condition

Condition:
Tagname: scm2 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: CM:Moderate :end
:end //of Condition

Condition:
Tagname: scm3 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: CM:Strong :end
:end //of Condition

Condition:
Tagname: OpsPhysec :end
ConditionClass: ZoneHasSecurityValue :end
ConditionText: Operations :end
Parameter: 400 :end
Parameter: 1000 :end
:end //of Condition

Condition:
Tagname: CompRoomPhysec :end
ConditionClass: ZoneHasSecurityValue :end
ConditionText: Computer room :end
Parameter: 400 :end
Parameter: 1000 :end
:end //of Condition

Condition:
Tagname: EntireOfficePhysec :end
ConditionClass: ZoneHasSecurityValue :end
ConditionText: Entire Office :end
Parameter: 300 :end
Parameter: 1000 :end
:end //of Condition

Condition:
Tagname: siprserverpw1 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Readiness Reports :end
SecondConditionText: PasswordLength:None :end
:end //of Condition

Condition:
Tagname: niprserverpw1 :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: PasswordLength:None :end
:end //of Condition

Condition:
Tagname: pwobjtrigger :end
ConditionClass: ObjectiveCompleted :end
ConditionText: pwpolicy :end
:end //of Condition

Condition:

Tagname: assetgoalsmet :end
Conditionclass: AllAssetGoalsMeet :end
:end //of Condition

Condition:
Tagname: ZeroCash :end
Conditionclass: MinCashOnHand :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: i21buy :end
Conditionclass: ObjectiveCompleted :end
ConditionText: NiprnetBoxes :end
:end //of Condition

Condition:
Tagname: i21physecentireoffice :end
Conditionclass: ObjectiveCompleted :end
ConditionText: PhyssecEntireoffice :end
:end //of Condition

Condition:
Tagname: i21physecsiprzones :end
Conditionclass: ObjectiveCompleted :end
ConditionText: PhyssecSiprZones :end
:end //of Condition

Condition:
Tagname: i21acl :end
Conditionclass: ObjectiveCompleted :end
ConditionText: ACL :end
:end //of Condition

Condition:
Tagname: avobj :end
Conditionclass: ObjectiveCompleted :end
ConditionText: antivirus :end
:end //of Condition

Condition:
Tagname: backupobj :end
Conditionclass: ObjectiveCompleted :end
ConditionText: backup :end
:end //of Condition

Condition:
Tagname: filteringobj :end
ConditionClass: ObjectiveCompleted :end
ConditionText: filtering :end
:end //of Condition

Condition:
Tagname: patchobj :end
ConditionClass: ObjectiveCompleted :end
ConditionText: patch :end
:end //of Condition

Condition:
Tagname: assetgoalsobjmet :end
ConditionClass: ObjectiveCompleted :end
ConditionText: Asset Goals Met :end
:end //of Condition

Condition:
Tagname: DACunclassserver :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: CrewEvaluationReports :end
SecondConditionText: ProtectWithACL: :end
:end //of Condition

Condition:
Tagname: DACsecretserver :end
ConditionClass: AssetComputerHasPolicy :end
ConditionText: Deployment Schedules :end
SecondConditionText: ProtectWithACL: :end
:end //of Condition

Condition:
Tagname: itstaffed :end
ConditionClass: ItSecStatus :end
Parameter: 0 :end
Parameter: 99 :end
:end //of Condition

Condition:
Tagname: JonesComputer :end
ConditionClass: UserHasAssignedComputer :end
ConditionText: SeamanJones :end
:end //of Condition

Condition:

Tagname: JonesInternet :end
Conditionclass: AssetToNetworkByFilterType :end
ConditionText: Jones' Stuff :end
SecondConditionText: Internet :end
ThirdConditionText: WEB SERVER :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: HewlettComputer :end
ConditionClass: UserHasAssignedComputer :end
ConditionText: ChiefHewlett :end
:end //of Condition

Condition:
Tagname: HewlettInternet :end
ConditionClass: AssetToNetworkByFilterType :end
ConditionText: Hewlett's Stuff :end
SecondConditionText: Internet :end
ThirdConditionText: WEB SERVER :end
Parameter: 0 :end
:end //of Condition

Condition:
Tagname: t1 :end
ConditionClass: TimeCondition :end
Parameter: 1 :end
Parameter: 1 :end
:end //of Condition

Condition:
Tagname: t10days :end
ConditionClass: TimeCondition :end
Parameter: 240 :end
Parameter: 1 :end
:end //of Condition

Condition:
Tagname: t20days :end
ConditionClass: TimeCondition :end
Parameter: 480 :end
Parameter: 1 :end
:end //of Condition

Condition:
Tagname: hewlettusageup :end

```
            ConditionClass: TriggerGoneOff :end
            ConditionText: hewlettstuffup :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

    Condition:
            Tagname: jonesusageup :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: jonesstuffup :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

    Condition:
            Tagname: assetgoalsobjoff :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: assetgoalobjcomp :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

    Condition:
            Tagname: itunderstaffedtickeroff :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: ITunderstaffed :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

    Condition:
            Tagname: filtertickeroff :end
            ConditionClass: TriggerGoneOff :end
            ConditionText: filterticker :end
            Parameter: 1 :end
            Parameter: 1 :end
:end //of Condition

    Condition:
            Tagname: viruspresent :end
            ConditionClass: VirusPresent :end
            ConditionText:  :end
:end //of Condition

    Condition:
            Tagname: onscrn :end
```

```
                ConditionClass: GameOnScreen :end
                Parameter: 2 :end
:end //of Condition

:end
Triggers:
        Trigger:
                TriggerName: deploymentsced :end
                TriggerClass: TickerTrigger :end
                FrequencyInDays: .1 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: false :end
                ConditionList: deploymentscedsattacked :end
                TriggerText: The deployment schedule has been attacked. :end
        :end //of Trigger

        Trigger:
                TriggerName: evalreports :end
                TriggerClass: TickerTrigger :end
                FrequencyInDays: .1 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: false :end
                ConditionList: evalreportsattacked :end
                TriggerText: The crew evaluations reports have been attacked.
:end
        :end //of Trigger

        Trigger:
                TriggerName: secretmauals :end
                TriggerClass: TickerTrigger :end
                FrequencyInDays: .1 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: false :end
                ConditionList: secretmanualsattacked :end
                TriggerText: The secret training manuals have been attacked. :end
        :end //of Trigger

        Trigger:
                TriggerName: readinessreports :end
                TriggerClass: TickerTrigger :end
                FrequencyInDays: .1 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
```

RunsWhilePaused: false :end
ConditionList: readinessreportsattacked :end
TriggerText: The readiness reports have been compromised. :end
:end //of Trigger

Trigger:
TriggerName: woodwardsstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: woodwardsstuffattacked :end
TriggerText: Woodward's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: packardstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: packardsstuffattacked :end
TriggerText: Packard's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: dellstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: dellsstuffattacked :end
TriggerText: Dell's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: gatesstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: gatesstuffattacked :end

TriggerText: Gate's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: torvaldsstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: torvaldsstuffattacked :end
TriggerText: Torvald's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: dewittsstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: dewittsstuffattacked :end
TriggerText: Dewitt's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: hewlettstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: hewlettstuffattacked :end
TriggerText: Hewlett's stuff has been compromised. :end
:end //of Trigger

Trigger:
TriggerName: jonesstuff :end
TriggerClass: TickerTrigger :end
FrequencyInDays: .1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: jonesstuffattacked :end
TriggerText: Jones' stuff has been compromised. :end
:end //of Trigger

```
Trigger:
        TriggerName: unmaskallattacks1 :end
        TriggerClass: MaskAttackTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: true :end
        ConditionList: endphase2 :end
        Parameter: -1 :end
        Parameter: 0 :end
:end //of Trigger

Trigger:
        TriggerName: i23attack5 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: true :end
        ConditionList: endphase2 :end
        TriggerText: OutsideTrojan5 :end
        Parameter: 5 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: i23attack17 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: true :end
        ConditionList: endphase2 :end
        TriggerText: InsiderHacking17 :end
        Parameter: 17 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: i23attack19 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: true :end
```

```
        ConditionList: endphase2 :end
        TriggerText: OutsiderInternet19 :end
        Parameter: 19 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: maskallattacks1 :end
        TriggerClass: MaskAttackTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase3 :end
        Parameter: -1 :end
        Parameter: 1 :end
:end //of Trigger

Trigger:
        TriggerName: unmaskallattacksphase5 :end
        TriggerClass: MaskAttackTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        Parameter: -1 :end
        Parameter: 0 :end
:end //of Trigger

Trigger:
        TriggerName: attack1 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 1 :end
        Parameter: 1 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack0 :end
        TriggerClass: AttackTrigger :end
```

```
        FrequencyInDays: 4 :end
        FixedDelay: .05 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 0 :end
        Parameter: 0 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack2 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .1 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 2 :end
        Parameter: 2 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack3 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .15 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 3 :end
        Parameter: 3 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack4 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .2 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 4 :end
        Parameter: 4 :end
```

```
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack5 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .25 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 5 :end
        Parameter: 5 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack6 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .3 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 6 :end
        Parameter: 6 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack7 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .35 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 7 :end
        Parameter: 7 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack8 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
```

```
        FixedDelay: .4 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 8 :end
        Parameter: 8 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack9 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .45 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 9 :end
        Parameter: 9 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack10 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: 0 :end
        RandomDelay: .5 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 10 :end
        Parameter: 10 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack11 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .55 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 11 :end
        Parameter: 11 :end
        Parameter: -2 :end
```

```
:end //of Trigger

Trigger:
        TriggerName: attack12 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .6 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 12 :end
        Parameter: 12 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack13 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .65 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 13 :end
        Parameter: 13 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack14 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 4 :end
        FixedDelay: .7 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 14 :end
        Parameter: 14 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack15 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 3 :end
        FixedDelay: .75 :end
```

```
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 15 :end
        Parameter: 15 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack16 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 3 :end
        FixedDelay: .8 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 16 :end
        Parameter: 16 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack17 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 3 :end
        FixedDelay: .85 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 17 :end
        Parameter: 17 :end
        Parameter: -2 :end
:end //of Trigger

Trigger:
        TriggerName: attack18 :end
        TriggerClass: AttackTrigger :end
        FrequencyInDays: 3 :end
        FixedDelay: .9 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase4 :end
        TriggerText: 18 :end
        Parameter: 18 :end
        Parameter: -2 :end
:end //of Trigger
```

```
Trigger:
	TriggerName: attack19 :end
	TriggerClass: AttackTrigger :end
	FrequencyInDays: 3 :end
	FixedDelay: .95 :end
	RandomDelay: 0 :end
	RunsWhilePaused: false :end
	ConditionList: endphase4 :end
	TriggerText: 19 :end
	Parameter: 19 :end
	Parameter: -2 :end
:end //of Trigger

Trigger:
	TriggerName: attack20 :end
	TriggerClass: AttackTrigger :end
	FrequencyInDays: 3 :end
	FixedDelay: .99 :end
	RandomDelay: 0 :end
	RunsWhilePaused: false :end
	ConditionList: endphase4 :end
	TriggerText: 20 :end
	Parameter: 20 :end
	Parameter: -2 :end
:end //of Trigger

Trigger:
	TriggerName: HewlettComputer :end
	TriggerClass: TickerTrigger :end
	FrequencyInDays: 999 :end
	FixedDelay: 0 :end
	RandomDelay: 0 :end
	RunsWhilePaused: true :end
	ConditionList: HewlettComputer :end
	TriggerText: Chief Hewlett has a computer. :end
:end //of Trigger

Trigger:
	TriggerName: JonesComputer :end
	TriggerClass: TickerTrigger :end
	FrequencyInDays: 999 :end
	FixedDelay: 0 :end
	RandomDelay: 0 :end
	RunsWhilePaused: true :end
	ConditionList: JonesComputer :end
```

TriggerText: Seaman Jones has a computer. :end
:end //of Trigger

Trigger:
TriggerName: AdminInternetAccessObj :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: JonesComputer And JonesInternet AND HewlettInternet AND HewlettComputer AND endphase3 :end
TriggerText: NiprnetBoxes :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: ACLObj :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: DACunclassserver AND DACsecretserver :end
TriggerText: ACL :end
SecondTriggerText: Now that you have enabled ACL's, don't forget to set them for the various assets on the bottom right of the components screen! :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: ACLunclassticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: DACunclassserver AND_NOT DACsecretserver :end
TriggerText: Your classified assets still need to have ACL's set. :end
:end //of Trigger

Trigger:
TriggerName: ACLsecretticker :end
TriggerClass: TickerTrigger :end

FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: DACsecretserver AND_NOT DACunclassserver :end
TriggerText: Your unclassified assets still need to have ACL's set
:end
:end //of Trigger

Trigger:
TriggerName: filteringobj :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: unclass2dmzemail AND niprlantodmzweb AND
dmz2internetweb AND dmztointernetemail AND_NOT dmz2internettelnet :end
TriggerText: filtering :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: filterticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: filteringobj :end
TriggerText: You have set up some filters for the internet. Don't
forget to tighten down the siprnet router. :end
:end //of Trigger

Trigger:
TriggerName: filterspeak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: filteringobj :end
TriggerText: LtRoberts :end
SecondTriggerText: FTP is a pretty insecure protocol. Did you
remember to tighten down all the routers? :end
:end //of Trigger

Trigger:
TriggerName: filterspeak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: filteringobj :end
TriggerText: LtRoberts :end
SecondTriggerText: You have set up some filters for the internet. Don't forget to tighten down the siprnet router. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: Physec :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: EntireOfficePhysec :end
TriggerText: PhyssecEntireoffice :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: physsecticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: EntireOfficePhysec :end
TriggerText: The entire office zone has been protected with some physical security mechanisms. :end
:end //of Trigger

Trigger:
TriggerName: SiprPhysec :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end

ConditionList: CompRoomPhysec AND OpsPhysec :end
TriggerText: PhyssecSiprZones :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: siprphyssecspeak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: CompRoomPhysec AND OpsPhysec AND onscrn :end
TriggerText: LtRoberts :end
SecondTriggerText: Are you sure that there are enough physical security mechanisms in place to protect the classified data? :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: pw :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: endphase1 AND_NOT siprserverpw1 AND_NOT niprserverpw1 :end
TriggerText: pwpolicy :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: pwticker :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: endphase1 AND_NOT siprserverpw1 AND_NOT niprserverpw1 :end
TriggerText: LtRoberts :end
SecondTriggerText: You have set some sort of password policy for the servers. :end
:end //of Trigger

```
        Trigger:
                TriggerName: antivirusobj :end
                TriggerClass: SetObjectiveStatus :end
                FrequencyInDays: 999 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: true :end
                ConditionList: endphase1 AND (niprserverav OR niprserverav2)
AND (siprserverav OR siprserverav2) :end
                TriggerText: antivirus :end
                Parameter: 1 :end
        :end //of Trigger

        Trigger:
                TriggerName: avobjspeak :end
                TriggerClass: SpeakTrigger :end
                FrequencyInDays: 999 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: true :end
                ConditionList: avobj AND onscrn :end
                TriggerText: LtRoberts :end
                SecondTriggerText: You have set the antivirus policy for the
servers. :end
                Parameter: 1 :end
        :end //of Trigger

        Trigger:
                TriggerName: avobjticker :end
                TriggerClass: TickerTrigger :end
                FrequencyInDays: 999 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: true :end
                ConditionList: avobj :end
                TriggerText: You have set the antivirus policy for the servers. :end
        :end //of Trigger

        Trigger:
                TriggerName: backupobj :end
                TriggerClass: SetObjectiveStatus :end
                FrequencyInDays: 999 :end
                FixedDelay: 0 :end
                RandomDelay: 0 :end
                RunsWhilePaused: true :end
```

ConditionList: endphase1 AND niprserverbackup AND siprserverbackup :end
ConditionList: backupobj AND onscrn :end
TriggerText: backup :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: backupspeak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: backupobj AND onscrn :end
TriggerText: LtRoberts :end
SecondTriggerText: You should configure the servers to be backed up by an administrator. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: patch :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: endphase1 AND (npatch OR npatch2 OR npatch3) AND (spatch OR spatch2 OR spatch3) AND (ncm1 OR ncm2 OR ncm3) AND (scm1 OR scm2 OR scm3) :end
TriggerText: patch :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: patch ticker :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: patchobj :end
TriggerText: You have set the configuration and patch options for the servers. :end
:end //of Trigger

Trigger:
TriggerName: patchspeak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: patchobj :end
TriggerText: LtRoberts :end
SecondTriggerText: You have configured the servers for patching.
:end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: assetgoals :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: assetgoalsobjoff and endphase3 :end
TriggerText: All asset goals have been met :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: assetgoalobjcomp :end
TriggerClass: SetObjectiveStatus :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: assetgoalsmet AND endphase3 AND
hewlettusageup AND jonesusageup AND i21buy :end
TriggerText: Asset Goals Met :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: woodwardreadinessusageup :end
TriggerClass: ChangeAssetUsageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end

ConditionList: endphase3 :end
TriggerText: LTjgWoodward :end
SecondTriggerText: ReadinessReportAccess :end
Parameter: 10 :end
:end //of Trigger

Trigger:
TriggerName: goalsunmet :end
TriggerClass: CashTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase4 AND_NOT assetgoalsmet :end
TriggerText: Not all the Asset goals are met. That $500 penalty due to work lost. :end
Parameter: -500 :end
:end //of Trigger

Trigger:
TriggerName: wiretap :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase4 AND t1 :end
TriggerText: LtRoberts :end
SecondTriggerText: Last week, one of the IT staff reported that they saw a "hub-like" device attached to the network. I'll be on the lookout for any "wiretapping" devices. :end
:end //of Trigger

Trigger:
TriggerName: hewletinternetup :end
TriggerClass: ChangeAssetUsageTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase3 :end
TriggerText: ChiefHewlett :end
SecondTriggerText: InternetAccess :end
Parameter: 15 :end
:end //of Trigger

```
Trigger:
        TriggerName: hewlettstuffup :end
        TriggerClass: ChangeAssetUsageTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase3 :end
        TriggerText: ChiefHewlett :end
        SecondTriggerText: Hewlett's Stuff :end
        Parameter: 15 :end
:end //of Trigger

Trigger:
        TriggerName: jonesinternetup :end
        TriggerClass: ChangeAssetUsageTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase3 :end
        TriggerText: SeamanJones :end
        SecondTriggerText: InternetAccess :end
        Parameter: 15 :end
:end //of Trigger

Trigger:
        TriggerName: jonesstuffup :end
        TriggerClass: ChangeAssetUsageTrigger :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: false :end
        ConditionList: endphase3 :end
        TriggerText: SeamanJones :end
        SecondTriggerText: Jones' Stuff :end
        Parameter: 15 :end
:end //of Trigger

Trigger:
        TriggerName: EndPhase1 :end
        TriggerClass: SetPhase :end
        FrequencyInDays: 999 :end
        FixedDelay: 0 :end
        RandomDelay: 0 :end
        RunsWhilePaused: true :end
```

ConditionList: i21physecentireoffice AND i21physecsiprzones AND I21acl AND filteringobj :end
TriggerText: 22 :end
:end //of Trigger

Trigger:
TriggerName: endphase1speak :end
TriggerClass: SpeakTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: i21physecentireoffice AND i21physecsiprzones AND I21acl AND filteringobj AND onscrn :end
TriggerText: LtRoberts :end
SecondTriggerText: You have completed the minimum to progress to phase 2. :end
Parameter: 1 :end
:end //of Trigger

Trigger:
TriggerName: EndPhase2 :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: endphase1 AND pwobjtrigger AND backupobj AND avobj AND patchobj :end
TriggerText: 23 :end
SecondTriggerText: Now that you have got a chance to set up your network, let's see how you did. Attacks will be unmasked for 1 hour to let the network vulnerability team assess your network. These attacks will cost you, but they will also give you a chance to fine-tune your system for the last phase. :end
:end //of Trigger

Trigger:
TriggerName: EndPhase3 :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase2 and t1 :end
TriggerText: 24 :end

SecondTriggerText: Was that so bad? Pause the game and complete the objectives for phase 4 and fix anything that phase 3 may have alerted you to. You will have to unpause the game to go to phase 5. :end
:end //of Trigger

Trigger:
TriggerName: EndPhase4 :end
TriggerClass: SetPhase :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase3 AND i21buy AND assetgoalsobjmet :end
TriggerText: 25 :end
SecondTriggerText: You have completed your objectives for phase 4. Are you ready to go operational? You can use "time compression" by hitting the c key. If you want to slow it down use capital C. :end
:end //of Trigger

Trigger:
TriggerName: pauseoperational :end
TriggerClass: HelpTipTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 1 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: onscrn AND_NOT endphase1 :end
TriggerText: Press this button only when you are ready to go operational. You can also press it to pause the game at any time. :end
Parameter: 300 :end
Parameter: 400 :end
Parameter: 765 :end
Parameter: 80 :end
:end //of Trigger

Trigger:
TriggerName: ITunderstaffed :end
TriggerClass: TickerTrigger :end
FrequencyInDays: 1 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: onscrn AND_NOT itstaffed :end
TriggerText: Your IT staff is staffed at less than 100%. You should hire more people. :end
Parameter: 0 :end

:end //of Trigger

Trigger:
TriggerName: ITunderstaffedpenalty :end
TriggerClass: CashTrigger :end
FrequencyInDays: 1 :end
FixedDelay: .01 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: itunderstaffedtickeroff AND_NOT itstaffed :end
TriggerText: Your IT staff is understaffed. This will cost your organization 500 dollars. :end
Parameter: -500 :end
:end //of Trigger

Trigger:
TriggerName: viruspresentmsg :end
TriggerClass: MessageTrigger :end
FrequencyInDays: .3 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase1 and viruspresent :end
TriggerText: There is malicious software on your computer network. This will cost you $1000.00. You should pause the game to find it and get rid of it before it spreads(unless it already has). You must use the remove software button to get rid of malware once you find it (Use the enclyclopedia for directions on how to get rid of malware). :end
:end //of Trigger

Trigger:
TriggerName: viruscost :end
TriggerClass: CashTrigger :end
FrequencyInDays: .3 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase1 and viruspresent :end
Parameter: -1000 :end
:end //of Trigger

Trigger:
TriggerName: 10daywin :end
TriggerClass: WinTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end

RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: endphase4 AND t10days :end
TriggerText: It has been 10 days. Your boss is back and is wondering what you spent all of that money on and why he can't get back into his office. You can check the game log to see what happened and what exactly got attacked. Auditing logs is something that a good system administrator will make time for. :end
:end //of Trigger

Trigger:
TriggerName: ZeroCashLoss :end
TriggerClass: LoseTrigger :end
FrequencyInDays: 999 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: true :end
ConditionList: ZeroCash :end
TriggerText: You spent all of your money! You lose. Try again. :end
:end //of Trigger

Trigger:
TriggerName: unathaccesstosipr :end
TriggerClass: CashTrigger :end
FrequencyInDays: .3 :end
FixedDelay: 0 :end
RandomDelay: 0 :end
RunsWhilePaused: false :end
ConditionList: SecretMantoNiprnet OR ReadinessReportNiprnet OR evalreportstosipr OR jonestosipr OR hewletttosipr OR dewitttosipr OR torvaldtosipr OR gatestosipr OR delltosipr OR packardtosipr OR woodwardtosipr :end
TriggerText: You connected an unclassified network to a classified network. After the investigation, you were severely reprimanded but not fired. But the investigation cost the command $100,000. :end
Parameter: -100000 :end
:end //of Trigger

:end
Filter:
ComponentDevice: INTERNET Gateway Router :end
Direction: BlockIn :end
SoftwareType: TELNET :end
NetworkAppliedTo: NiprLan :end
:end //Filter

Filter:
ComponentDevice: SIPRNET Gateway Router :end
Direction: BlockBothDirections :end
SoftwareType: TELNET :end
SoftwareType: FTP :end
SoftwareType: SSH :end
SoftwareType: DATABASE :end
SoftwareType: DEFENSE RAT :end
SoftwareType: DEFENSE 4T :end
SoftwareType: REPORTING :end
SoftwareType: MANAGEMENT :end
SoftwareType: INTERNAL IP ADDRESSES :end
NetworkAppliedTo: SIPRNET :end
:end //Filter

Filter:
ComponentDevice: InternetRouters :end
Direction: BlockBothDirections :end
SoftwareType: TELNET :end
SoftwareType: FTP :end
SoftwareType: SSH :end
SoftwareType: DATABASE :end
SoftwareType: DEFENSE RAT :end
SoftwareType: DEFENSE 4T :end
SoftwareType: REPORTING :end
SoftwareType: MANAGEMENT :end
SoftwareType: INTERNAL IP ADDRESSES :end
SoftwareType: EMAIL SERVER :end
SoftwareType: VPN GATEWAY :end
NetworkAppliedTo: OffsiteNetworks :end
:end //Filter

Phases:
Phase:
TagName: 21 :end
DisplayName: Physical Security, Filtering, and Access Control :end
CompletedText: :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

Phase:
TagName: 22 :end
DisplayName: Password Policies, Anti-Virus, Network Management Decision-Making, Offsite Backups :end
CompletedText: :end

UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

Phase:
TagName: 23 :end
DisplayName: Network Vulnerability Assessment :end
CompletedText: :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

Phase:
TagName: 24 :end
DisplayName: Configuring New Computers to Existing Infrastructure, Review Security Posture :end
CompletedText: :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

Phase:
TagName: 25 :end
DisplayName: Going Operational and Managing the Onslaught of Attacks :end
CompletedText: :end
UncompletedText: :end
PhaseCompleted: False :end
:end //of Phase

:end
Objectives:
Objective:
TagName: ACL :end
DisplayName: :end
Phase: 0 :end
ObjectiveCompleted: false :end
LastPhase: 0 :end
CompletedText: Even though some users have the necessary classification to see these assets, you set up a discretionary access control(DAC) mechanism to keep access to only those that needed to have access(the individual departments). :end
UncompletedText: There are several assets on the SECRET AND UNCLASS servers that are open to all users on that system (Public group). This is a situation where Discretionary Access Control (DAC) would be appropriate. Protect these assets by using ACL's (Access Control Lists) to reflect the asset's

intended access. If the wrong ACL's are set and someone not on the intended access list gains access, it may cost you later in the game. The minimum work necessary to complete this objective is to set the proper procedural setting for the two servers. This will ensure that the assets will be protected with ACL's. :end
:end //of Objective

Objective:
TagName: NiprnetBoxes :end
DisplayName: :end
Phase: 3 :end
ObjectiveCompleted: false :end
LastPhase: 3 :end
CompletedText: Chief Hewlett and Seaman Jones are connected to the Ship's network :end
UncompletedText: Buy the admin department two desktops. Assign one to Seaman Jones and the other to Chief Hewlett (hint: drop them on the two empty desks). Connect them to the Niprlan Network to get them email and Internet access. Configure them appropriately for the next phase when you go operational!(Hint: You may have to momentarily unpause the game to test connectivity) :end
:end //of Objective

Objective:
TagName: filtering :end
DisplayName: :end
Phase: 0 :end
ObjectiveCompleted: false :end
LastPhase: 0 :end
CompletedText: You have complied with your command's security regulation regarding the use of telnet, feel free to adjust all the routers as you see fit. :end
UncompletedText: Set up filters on the Internet Gateway router and the niprlan2dmz router. You must ensure that users on the niprlan have access to shared resources on the unclassdmz as well as internet access(both web and email). To complete this objective, you must prevent telnet access between the Internet and the Unclasssmz networks while ensuring email and web access to the Internet. This is to comply with the security regulations for your command (hint: The principle of least privilege is appropriate here, use your initiative.) If you have trouble finding the routers, use the network tab and find them on the network schematic. :end
:end //of Objective

Objective:
TagName: PhyssecEntireoffice :end
DisplayName: :end
Phase: 0 :end

ObjectiveCompleted: false :end
LastPhase: 0 :end
CompletedText: We'll see how good the physical security is for the entire office in the next few phases...feel free to tighten it up more. :end
UncompletedText: Your boss has directed you to increase the level of physical security in the entire office to at least 300 (You may have to momentarily unpause the game to verify completion). :end
:end //of Objective

Objective:
TagName: pwpolicy :end
DisplayName: :end
Phase: 1 :end
ObjectiveCompleted: false :end
LastPhase: 1 :end
CompletedText: Your have set password policies on the servers. :end
UncompletedText: Set password policies for the 2 servers. This may also be a good time to review the settings for the rest of the computers in the command.(Hint: If a password is too simple or does not need to be changed very often, it is easy for hackers to crack. If a password is too complex and needs to be changed too often, then users will be more likely to undermine this security measure.) :end
:end //of Objective

Objective:
TagName: patch :end
DisplayName: :end
Phase: 1 :end
ObjectiveCompleted: false :end
LastPhase: 1 :end
CompletedText: The servers have a patching configuration. :end
UncompletedText: Computers need to be updated with patches from time to time. Set the patching configuration you feel most comfortable with on the two servers. There are three different configurations each with particular advantages and disadvantages. With regular updates, there is a window of opportunity for an attacker to find a hole in your system before it is patched, but you can test the patch to ensure that it will not crash your network. With “automatic” or “as released” updates, it is harder for an attacker to exploit the window of opportunity provided by an unpatched system, but you give up the ability to test compatibility with your network or computer architecture. You also give up the ability to control when your systems are patched. After you configure patching updates, set the configuration management settings you feel most comfortable with on the servers. :end
:end //of Objective

Objective:

TagName: PhyssecSiprZones :end
DisplayName: :end
Phase: 0 :end
ObjectiveCompleted: false :end
LastPhase: 0 :end
CompletedText: Your Zones with siprnet access have a higher level of protection. :end
UncompletedText: You have two zones with SIPRNET access. Identify these two zones and increase the level of physical security in the areas with siprnet drops to 400. The more you spend, the more security you will have, but if it gets excessive, you may lose employee happiness and productivity which will contribute to your success... Hint: You need to hire IT staff(security) for the guards present or roaming options to increase your security. :end
:end //of Objective

Objective:
TagName: Review Settings :end
DisplayName: Review all the security settings for your network. You will have to go operational for at least 1 hour to pass phase 3. This will give you an indication if there are any MAJOR holes that you will need to fix before phase 5. :end
Phase: 1 :end
ObjectiveCompleted: false :end
LastPhase: 1 :end
CompletedText: :end
UncompletedText: :end
:end //of Objective

Objective:
TagName: antivirus :end
DisplayName: :end
Phase: 1 :end
ObjectiveCompleted: false :end
LastPhase: 1 :end
CompletedText: You have set Anti-virus updating policy for the servers. :end
UncompletedText: The servers do not have any Anti-Virus procedures set. You need to choose between regular or automatic updates, both of which have advantages and disadvantages similar to those described for patches. :end
:end //of Objective

Objective:
TagName: backup :end
DisplayName: :end
Phase: 1 :end
ObjectiveCompleted: false :end

LastPhase: 1 :end
CompletedText: Since servers have resources that are generally shared, it is better if they have admin backups. :end
UncompletedText: Store the backups from both servers off-site in order to ensure that these assets are recoverable during various contingencies. :end
:end //of Objective

Objective:
TagName: testing :end
DisplayName: You must allow the game to run for 1 hour of game time to see if they are any major holes in your network. Do not be convinced that you have an impregnable network if no attacks occur. When you go operational in phase 5, there will be those who will attack your network with no mercy. Feel free to use the "c" option to compress the game time (Hint: Don't forget to unpause and pause the game). :end
Phase: 2 :end
ObjectiveCompleted: false :end
LastPhase: 2 :end
CompletedText: :end
UncompletedText: :end
:end //of Objective

Objective:
TagName: Asset Goals Met :end
DisplayName: :end
Phase: 3 :end
ObjectiveCompleted: false :end
LastPhase: 3 :end
CompletedText: All of the Asset goals were met. :end
UncompletedText: You must ensure that all of the asset goals are met for all users before progressing to Phase 5 (Hint: You may have to unpause the game momentarily for the game to verify completion of this objective. Check each user for asset failures using the user tab). :end
:end //of Objective

Objective:
TagName: securitysettings :end
DisplayName: :end
Phase: 3 :end
ObjectiveCompleted: false :end
LastPhase: 3 :end
CompletedText: :end
UncompletedText: You should review all the security settings for your network before phase 5. This is always a good idea before you take things operational. (Hint, check the component access list for one of the servers just to make sure everyone has a "need to know") :end

:end //of Objective

Objective:
TagName: 10daysurvival :end
DisplayName: :end
Phase: 4 :end
ObjectiveCompleted: false :end
LastPhase: 4 :end
CompletedText: You're done! :end
UncompletedText: You must allow the game to run for 10 days of game time. During this time, you can pause the game at any time to adjust your settings if you get attacked. :end
:end //of Objective

:end
ShortBriefing:
Your boss, the Command Security Coordinator had to go out of town for 10 days. He left you with the task of managing the security of the computer network and achieving the IT objectives for the Command. His biggest concern was that both servers needed some attention and that the Admin department desperately needs two computers. He left you in charge of three internal networks, one of which handles classified information (siprlan) and is connected to the SIPRNET. He left you a list of things to do in the form of objectives. Your task will be to secure the network while staying within budget and achieving your objectives. You will have a chance to test your security measures for one hour of game time to fine tune your settings in the middle of the scenario. During the last portion of the scenario, you will have to let your network go operational for at least 10 days of game time until your boss gets back. Good luck and don't go broke!
:end

Briefing:
Your boss, the Command Security Coordinator had to go out of town for 10 days. He left you with the task of managing the security of the computer network and achieving the IT objectives for the Command. His biggest concern was that both servers needed some attention and that the admin department desperately needs 2 computers. He left you in charge of 3 internal networks, one of which handles classified information (siprlan) and is connected to the Siprnet. He left you a list of things to do in the form of objectives. Your task will be to secure the network while staying in budget and achieving your objectives. Phase 3 will give you a chance to test your security measures for 1 hour of game time to fine tune your settings. During phase five, you will have to let your network survive for at least 10 days of game time until your boss gets back. Good luck and don't go broke! (PARAGRAPH) After completing the IA technical-level training scenario, a typical information system administrator should be able to: (PARAGRAPH) 1. Identify the purpose of access control. (PARAGRAPH) 2.

Identify the need for regular backups of important data. (PARAGRAPH) 3. Describe various criteria for passwords and determine their effect on password management. (PARAGRAPH) 4. Describe the function of anti-virus tools. (PARAGRAPH) 5. When given a physical layout, be able to identify physical control mechanisms that will enhance the overall security. (PARAGRAPH) 6. Describe the function of various network devices and interfaces. (PARAGRAPH) 7. Describe basic computer and network security mechanisms. (PARAGRAPH) 8. Describe some issues associated with updating software. (PARAGRAPH) 9. Describe methods for security policy enforcement. (PARAGRAPH)
:end

:EndOfFile

LIST OF REFERENCES

[CSA 1987] Public Law 100-235, "The Computer Security Act of 1987."

[DISA1 2004] Defense Information Systems Agency "DOD Information Assurance Awareness" CBT Version 2.0, December 2004.

[DISA2 2005] Defense Information Systems Agency Information Assurance Branch. "Information Assurance Security Awareness Briefing." Available from http://iase.disa.mil/ia-awareness-training.pdf; Internet; accessed November 1, 2005.

[DOD 2004] DOD Directive 8570.1. "Information Assurance Training, Certification, and Workforce Management." August 15, 2004.

[FISMA 2002] Federal Information Security Management Act of 2002. Available from http://csrc.nist.gov/policies/FISMA-final.pdf; Internet; accessed December 30, 2005.

[Irvine 2005] Irvine, C.E., Thompson, M.F., and Allen, K. *CyberCIEGE: Gaming for Information Assurance*. IEEE Security and Privacy, (May/June 2005), Volume 3 Issue 3, 61-64.

[Irvine2 2003] Irvine, C.E., Thompson, M.F., *Teaching Objectives of a Simulation Game for Computer Security*, Proceedings of the Informing Science and Information Technology Joint Conference, Pori, Finland, June 24-27, 2003.

[Irvine3 1998] Irvine, C.E., Chin S., Frincke D. *Integrating Security into the Curriculum*. IEEE Computer, December 1998, 25-30.

[Joint 1998] Joint Publication 3-13. "Joint Doctrine for Information Operations." 9 October 1998.

[Mitnick 2002] Mitnick, Kevin. *The Art of Deception*. Wiley, Indianapolis IN, 2002.

[Murray 2005] Murray, W. H. Course Lecture in CS3670, Secure Management of Systems, Naval Postgraduate School. March 2005.

[NIST1 1998] NIST Special Publication 800-16. “Information Technology Security Training Requirements: A Role- and Performance-based model.” April 1998.

[NIST2 2003] NIST Special Publication 800-50. “Building an Information Technology Security Awareness and Training Program.” October 2003.

[NAVSO1 1995] Navy Staff Office Publication 5239-04. “Information Systems Security Manager (ISSM) Guidebook.” September, 1995.

[NAVSO2 1996] Navy Staff Office Publication 5239-07. "Information Systems Security Officer (ISSO) Guidebook." February, 1996.

[NAVSO3 1996] Navy Staff Office Publication 5239-08. "Network Security Officer (NSO) Guidebook." March 1996.

[NAVY1 1999] Secretary of the Navy Instruction 5510.36. Department of the Navy (DON) Information Security Program (ISP) Regulation. 17 March 1999.

[Navy2 2004] Secretary of the Navy Instruction 5239.3A. “Department of the Navy Information Assurance (IA) policy.” 20 December 2004.

[Older 2003] Older, S. “Outcome-based Assessment as an Assurance Tool.” *Security Education and Critical Infrastructures,* Kluwer Academic Publishers, Norwell, Mass, 2003, 179-196.

[Ruppar 2005] Ruppar, C. A. *Identity Theft Prevention In CyberCIEGE*. Masters of Science Thesis, Department of Computer Science, Naval Postgraduate School. December 2005.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Ken Allen
   Rivermind, Inc
   Mountain View, CA

4. Hugo A. Badillo
   NSA
   Fort Meade, MD

5. George Bieber
   OSD
   Washington, DC

6. RADM Joseph Burns
   Fort George Meade, MD

7. John Campbell
   National Security Agency
   Fort Meade, MD

8. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

9. CDR Daniel L. Currie
   PMW 161
   San Diego, CA

10. Louise Davidson
    National Geospatial Agency
    Bethesda, MD

11. Steve Davis
    NRO
    Chantilly, VA

12. Vincent J. DiMaria
National Security Agency
Fort Meade, MD

13. LCDR James Downey
NAVSEA
Washington, DC

14. Scott Gallardo
Rivermind, Inc
Mountain View, CA

15. Dr. Diana Gant
National Science Foundation

16. Jennifer Guild
SPAWAR
Charleston, SC

17. Richard Hale
DISA
Falls Church, VA

18. CDR Scott D. Heller
SPAWAR
San Diego, CA

19. Willis Janssen
CTO, ASDS&CI
Huntingtown, MD

20. Wiley Jones
OSD
Washington, DC

21. Russell Jones
N641
Arlington, VA

22. David Ladd
Microsoft Corporation
Redmond, WA

23. Dr. Carl Landwehr
DTO
Fort George T. Meade, MD

24. Steve LaFountain
NSA
Fort Meade, MD

25. Dr. Greg Larson
IDA
Alexandria, VA

26. Paul Livingtson
DNI
Washington, DC

27. Gilman Louie
In-Q-Tel
Menlo Park, CA

28. Mark T. Powell
Federal Aviation Administration
Washington, DC

29. CAPT Deborah McGhee
Headquarters U.S. Navy
Arlington, VA

30. Dr. Vic Maconachy
NSA
Fort Meade, MD

31. Doug Maughan
Department of Homeland Security
Washington, DC

32. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

33. John Mildner
SPAWAR
Charleston, SC

34. Jim Roberts
Central Intelligence Agency
Reston, VA

35. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

36. Charles Sherupski
Sherassoc
Round Hill, VA

37. Dr. Ralph Wachter
ONR
Arlington, VA

38. David Wennergren
DoN CIO
Arlington, VA

39. David Wirth
N641
Arlington, VA

40. Jim Yerovi
NRO
Chantilly, VA

41. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

42. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

43. Dr. Nelson J. Irvine
Naval Postgraduate School
Monterey, CA

44. Michael Thompson
Naval Postgraduate School
Monterey, CA

45. Benjamin D. Cone
Naval Postgraduate School
Monterey, CA