NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERCIEGE SCENARIO ILLUSTRATING SECRECY ISSUES THROUGH MANDATORY AND DISCRETIONARY ACCESS CONTROL POLICIES IN A MULTI-LEVEL SECURITY NETWORK

by

Robert L. LaMore

June 2004

Thesis Co-Advisor:	Cynthia Irvine
Thesis Co-Advisor:	Paul Clark
Second Reader:	Mike Thompson

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** June 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: CyberCIEGE Scenario Illustrating Secrecy Issues Through Mandatory and Discretionary Access Control Policies in a Multi-Level Security Network			**5. FUNDING NUMBERS**
6. AUTHOR(S) Robert L. LaMore			
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)

User training in computer and network security is crucial to the survival of modern networks, yet the methods employed to train users often seem ineffective. One possible reason is that users are not fully engaged during these training sessions and thus they tend to forget the lessons being taught.

The CyberCIEGE game introduces a new method of training in computer and network security. The player engages in a simulation-based network security game, that reflects real-world security principles. Each time the CyberCIEGE game runs, it loads a *Scenario Definition File (SDF)* written to teach specific security concepts.

This thesis developed such a scenario definition file for the CyberCIEGE game. The educational purpose of the scenario is to illustrate secrecy issues in the context of mandatory and discretionary access control in a multilevel networked environment. The primary work of this thesis was to construct the scenario definition file such that playing the resulting game would achieve this educational purpose.

This thesis also resulted in the construction of scenario definition files to test the CyberCIEGE game engine for expected results. These tests resulted in several recommendations for improvement in the game engine.

14. SUBJECT TERMS Information Assurance, CyberCIEGE, Scenario Definition File, Network Security Training			**15. NUMBER OF PAGES** 210
			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.

CYBERCIEGE SCENARIO ILLUSTRATING SECRECY ISSUES THROUGH MANDATORY AND DISCRETIONARY ACCESS CONTROL POLICIES IN A MULTI-LEVEL SECURITY NETWORK

Robert L. LaMore
First Lieutenant, United States Air Force
B.S., Austin Peay State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
June 2004

Author: Robert L. LaMore

Approved by: Cynthia Irvine
Thesis Co-Advisor

Paul Clark
Thesis Co-Advisor

Mike Thompson
Second Reader

Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

User training in computer and network security is crucial to the survival of modern networks, yet the methods employed to train users often seem ineffective. One possible reason is that users are not fully engaged during these training sessions and thus they tend to forget the lessons being taught.

The CyberCIEGE game introduces a new method of training in computer and network security. The player engages in a simulation-based network security game, that reflects real-world security principles. Each time the CyberCIEGE game runs, it loads a *Scenario Definition File (SDF)* written to teach specific security concepts.

This thesis developed such a scenario definition file for the CyberCIEGE game. The educational purpose of the scenario is to illustrate secrecy issues in the context of mandatory and discretionary access control in a multilevel networked environment. The primary work of this thesis was to construct the scenario definition file such that playing the resulting game would achieve this educational purpose.

This thesis also resulted in the construction of scenario definition files to test the CyberCIEGE game engine for expected results. These tests resulted in several recommendations for improvement in the game engine.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express thanks to many individuals without whom the completion of thesis would not be possible.

I give thanks to my wife and children. Your unwavering support provided the strength I needed so desperately through the entire thesis process.

I would like to thank Dr. Cynthia Irvine, Paul Clark, and Mike Thompson, my advisory team. Thank you for your patience, especially when I struggled to grasp the concepts involved with this thesis.

I would also like to extend a special thank you to Marc Meyer, Justin Lamorie, and Klaus Fielk. Your willingness to share ideas and lend a helping hand have been an inspiration to me. I will never forget your contributions during this long process.

Finally, I would also like to thank Chris Lapacik, Gary Kreeger, and Jean Brennen for your absolutely fantastic job of supporting me as a student through my academic career at NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION AND BACKGROUND

A. THESIS STATEMENT

The purpose of this thesis is to develop Scenario Definition Files (SDF's) for the Naval Postgraduate School's CyberCIEGE project. The CyberCIEGE game uses these SDF's to control the player's game play experience. The purpose of the scenarios is education and training in Information Assurance topics related to a networking environment. The focus area of the scenarios is the protection of secrets in a multilevel network on a military installation. In addition, the scenario definition files will be used to test and evaluate the CyberCIEGE game engine for expected results. The impact of this research could have far reaching benefits for future United States Air Force (USAF) and Department of Defense (DoD) training and education requirements in the Information Assurance and Network Security arena.

B. THESIS SCOPE AND LAYOUT

This thesis develops a scenario definition file to illustrate secrecy issues in the context of mandatory and discretionary access control mechanisms in a multilevel networked environment. This thesis will also develop a test plan to validate whether the CyberCIEGE game engine produces expected results from a specified scenario definition file.

The thesis chapters will be organized as follows:

Chapter I - Introduction and Background – This chapter introduces the CyberCIEGE game and explains the motivation behind this thesis.

Chapter II - Scenario Goals – This chapter explains the objectives and educational goals associated with the scenario being developed for this thesis.

Chapter III - Scenario Outline – This chapter discusses the various components of the scenario definition file.

Chapter IV - Test Plan – This chapter describes the testing accomplished to validate the expected game engine results.

Chapter V - Conclusion and Recommendations – This chapter summarizes the conclusions reached and makes recommendations for future work.

C. BACKGROUND

1. Project Background

One of the more daunting security challenges facing network administrators today is that of user training. It does not matter how much the perimeter of the network has been hardened. It only takes a single inept user to create all sorts of security nightmares. If the user can access the Internet from behind the company firewall, then the entire network is only as safe as that user's level of training and security awareness. Companies spend massive amounts of budgeted dollars attempting to train their users in computer and network security (as much as $761 per employee annually according to the American Society for Training and Development [ASTD]), with limited return on those dollars. Why? Even if the training was effective for 99 out of 100 users, it only takes the actions of that last user to either, in the best case, leave the network vulnerable to a host of threats, or in the worst case, cripple and destroy sensitive networks and data.

Even though user training is crucial to the survival of modern networks, the methods employed to train users often seem ineffective. The standard methods for user training are: seminar and classroom-style settings where users are given lectures about such topics as the importance of good passwords and other security procedures, memoranda from security officers about the seriousness of network security in the organization; and computer-based training which is often little better than reading a few paragraphs and looking at pictures. Because users are not fully engaged during these training sessions, they tend to forget the lessons being taught.

The average users comprise only one group in need of better training. Senior managers and leaders also need to be conversant in the realm of security. Organizations rely on these individuals to make rational decisions regarding organizational security policies. Members of management need to understand the impact their decisions will

have on the networks they are responsible to keep secure. An organization's emphasis on security will only be as strong as its leadership's personal commitment to following good computing practices. Average users will not take seriously any suggestions to change in their bad habits if they do not see their superiors doing the same.

Managers need to be trained to make good security decisions when acquiring and deploying new technologies. They need to ask vendors about the assurance level of new systems. They need to be able to discuss mechanisms in the operating systems that enforce the security policy. The manager cannot risk network compromise due to ignorance of security issues.

Current methods used to train managers in security are: self-initiated education through reading articles relevant to specific network security topics; informal peer-to-peer sharing of security lessons learned; attendance at conferences and seminars that provide overviews of many security topics but no in-depth coverage of any specific one; and participation in courses designed to certify the manager in a specific application such as network administration on a specific platform. Because of the large number of security issues facing managers, they can lose sight of those that are most critical to their organization.

In the face of these challenges the way security training is accomplished needs to be re-examined. Effective training is vital to the security and availability of networks today.

2. CyberCIEGE

CyberCIEGE was specifically created to introduce a new method of training in network security. The driving force behind the CyberCIEGE game is the idea that security can be taught and the concepts better retained by the users if it is presented in an entertaining manner. The user then becomes a player who is invited to sit down and play a simulation-based network security game, that reflects real-world security principles. The player can take on the role of a network administrator and can attempt to protect his assets from threats, vulnerabilities, and attack.

Each time the game runs, it loads a *Scenario Definition File (SDF)* which has been written in the *Scenario Definition Language*. The designer of the SDF writes the scenario so that as the user progresses through game play, he is actually learning the specific security concepts intended by that scenario.

The CyberCIEGE game attempts to model most real-world types of security threats. If the network is connected to the Internet, hackers may gain access to confidential data. The network could suffer a Denial of Service (DoS) attack, rendering the networks unavailable and unusable to the users. Physical security is also taken into consideration. Unwanted outsiders may steal physical machines if they are not properly secured. Insider threats are addressed as well. Disgruntled employees may sell secrets to outside interests and compromise well guarded assets. And finally, user training is illustrated through the game as well. Poorly trained users will not properly follow intended security procedures and will then create vulnerabilities which will be exploited by those with malicious intent.

This thesis will develop a scenario definition file for the CyberCIEGE game. The purpose of the scenario will be to illustrate secrecy issues in the context of mandatory and discretionary access control mechanisms in a multilevel networked environment.

Before the scenario can be written, an understanding of these mechanisms must be developed. What is meant by mandatory access control and discretionary access control and what is the difference between them? What is a multilevel networked environment? What is meant by secrecy and what are the issues associated with it? It is not in the scope of this thesis to completely describe all aspects of these mechanisms, but rather to provide the basic groundwork upon which the training goals of the scenario will be built. Each of the following sections explores the ideas that the scenario is intended to teach.

3. Security

A working definition of the term computer security is needed. Many papers and books have covered this topic. For the purposes of this thesis, the definition of security used by Brinkley and Schell will suffice. According to their paper, the cornerstone

characteristics of network security are summarized in three key words [Brinkley]: Confidentiality, Integrity, and Availability.

Confidentiality is related to the idea of preventing unauthorized disclosure. Certain things must be kept secret. Whether it is the formula for a popular carbonated beverage, or the location of a certain military facility, an organization's secrets must remain so or risk the loss of its livelihood. A hospital keeps its medical records on its patients confidential. Individuals cannot walk into the administrative area of the hospital and simply start reading other people's records. The hospital implements certain procedures to ensure that only authorized disclosure occurs. But that same hospital probably is also connected to the Internet. What measures are taken to prevent disclosure to hackers? According to a CNN article in December of 2000 [CNN], a Seattle hospital had 5,000 of its patients' records illegally copied by a hacker. USAToday reported in April 2003 [USATODAY] that a small hospital outside of Reno, NV had its network accessed by a Russian hacker. Because hospitals are prime targets for hackers today, they must be careful to maintain the good network security practices that will ensure the privacy of its patient records.

The second key word is integrity. This relates to controls to ensure that unauthorized modification of information has not occurred. Continuing with the hospital example from above, once an intruder has gained access to a hospital's network, what other damage could be done besides obtaining copies of confidential records? Wouldn't it be just as easy for the hacker to alter patient records? What if the hacker decided to change drug dosages for patients? He could erase records of patients' allergic reactions to certain medications. The potential for great harm to human life abounds in this scenario.

Finally, the third key word is availability. This concept deals with keeping computer and network resources available to users. A generic term for Internet attacks on availability is a Denial of Service (DoS) attack. The attacker directs certain types of network traffic at his target in the hope of overwhelming its networks and denying its use for the duration of the attack. A company that relies on Internet commerce as its source of revenue could find itself losing money quickly when one of these attacks takes place. An

informed manager keeps up with the latest security threats and countermeasures and uses them to protect his organization from DoS attacks.

Brinkley and Schell [Brinkley] go on to describe important distinctions among these three ideas. The first is the differentiation of availability from integrity and confidentiality. Whereas the latter two deals exclusively with data stored on various resources, availability also encompasses the resources themselves. Protecting information from unauthorized disclosure or modification is accomplished solely by preventing unwanted access. Not so with availability. Not only is there a potential of outside attackers causing a DoS attack, but there is also the potential for processes running on network machines to interrupt network availability as well. In fact, the number and kinds of disruption are so great, that it is impossible to account for them all. Due to its subjective nature, the fact remains that it is impossible to guarantee availability in the general sense.

Aggravating this situation is the introduction of malicious software. Viruses, worms, Trojan horses, logic bombs, keyloggers, backdoors, and other mechanisms are also possible means of denying availability, as well as violating confidentiality and integrity. High assurance systems undergo rigorous development to ensure that none of these types of software are present within the protection mechanisms themselves. But this security engineering only raises assurance in the protection mechanisms; it does not absolutely guarantee the non-existence of such programs outside of the protection mechanisms. Integrity and confidentiality policies can be implemented with a higher degree of assurance using mathematical tools and formal methods to demonstrate that the policies are enforced regardless of the actions taken by software external to the protection mechanisms. This does not apply to availability, which is subjective. The organization relies heavily on the training and continuing education of its security manager to know how to safeguard from attacks on availability.

4. Security Policy

Training top level management and decision makers in computer security is another key to a successful security program. Any organization possessing information technology is vulnerable to the threats associated with using that technology.

Management cannot ignore these issues. Rather, they must face these issues head on and present a clear vision and strong example that the organization can follow.

Management must start with a carefully articulated, coherent security policy. This should be a short one to three page statement describing the organization's intentions with respect to the security of its networks. A well written security policy will set forth "the laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information" [Brinkley]. It is important to avoid specifying actual names of individuals in the policy document. Rather, state the access required by holders of positions. For instance, rather than stating that General Halftrack requires access to certain information, the policy should state that the base commander requires access to that information. This prevents rewriting the security policy every time individuals change position within the organization. The focus of the policy is to define desired behavior in the computer systems and networks the organization is responsible for protecting.

According to Sterne [Sterne], the following objectives should be kept in mind when designing a security policy:

"Distinguish policies that govern human behavior from those that govern automated subjects; and clarify the relationship between these two levels of abstraction."

"Distinguish security policies from other kinds of critical requirements."

"Provide the basis for comparing and distinguishing between different classes of integrity and assured service requirements."

"Define a generalized view of security that is a conservative extension of established concepts, and appears tractable in part, by application of current computer security principles and technology."

"The policy concerns itself with preventing and protecting against active (human) threats, rather than recovering from natural disaster." [Sterne].

A typical security policy will define security classes. This allows individuals holding certain clearances access to data classified at that level. The military uses security clearances in this manner. Information may be labeled as “Unclassified” meaning that no clearance is required to access that particular information. Other security labels include “Confidential”, “Secret”, and “Top Secret.” An order among these classes is also implied. If a user possesses a Secret clearance, it is understood that he is also cleared to access data at a lower level such as Confidential.

While the military model concerns itself mostly with preserving confidentiality, commercial sector companies may also be concerned with maintaining integrity. Clark and Wilson discuss important differences in approaches to security between the private and military sectors in their paper, “A Comparison of Commercial and Military Computer Security Policies” [Clark]. They state that commercial companies may be more concerned with internal fraud and errors than with unintended disclosure. In this case, more emphasis would be placed on integrity policies versus confidentiality. It is vital for the key decision makers in any organization to determine exactly which security properties are appropriate to their situation and tailor the policy accordingly.

Do not confuse the policy with the mechanism. The policy is nothing more than a statement of intentions or rules. Mechanisms are placed into systems which implement the policy. System designers must map these mechanisms back to the policy to show that they indeed implement what was stated.

5. Access Control Policies

As stated above, a distinction must be made between a security policy and a security mechanism. The mechanism is used within a system to uphold the policy. The same distinction can be made for access control. An access control policy can be used as an extension of an access related security policy. It defines the actual rules to enforce the security policy in the system. The underlying mechanisms in turn take these rules and enforce them. In the network security arena, these mechanisms are included in the Trusted Computing Base (TCB) [Brinkley]. The TCB is the entire spectrum of functions that implement the security policy. The goal of security engineering is to create functions in the TCB which correspond to each aspect of the security policy.

Access control policy can be further subdivided into two categories: mandatory and discretionary. A particular user may be permitted to exercise discretionary control over the files that he has created. He may allow others to read, write, or modify these files while maintaining control over who has access. This is discretionary access control. The user has the authority to grant or revoke permissions to files of which he is the owner.

On the other hand, the users of the network may be bound by system controls based on security clearances as to which resources they are allowed to access. Each file and program has associated with it a security label. Only subjects with a security label that dominates the object's security label are allowed access to these files and program. This system enforcement of access is mandatory access control.

Why are mandatory access control policies so important? A major reason is to prevent damage from malicious software, whether it is intentionally installed on the system or not. Mandatory access control prevents the unauthorized flow of information from one security class to another. By limiting these information flows, damage from malicious software is contained. For example, if User X introduces a Trojan horse into the system, then that software will only be allowed to execute with the same privileges as User X. This prevents the Trojan horse from writing higher sensitivity data to a lower sensitivity file or from reading higher sensitivity data. This minimizes the amount of damage that would be caused by the Trojan horse.

6. Mandatory Access Control Policy

Mandatory access control mechanisms are put into place to implement the mandatory access control policy. These mechanisms enforce the mandatory policy by restricting which subjects are allowed access to which objects. In this case, subjects represent users and the objects might be files. Subjects can also be processes started by users, which require access to objects. They can even be processes created by other processes. With mandatory access control, system owners can have a high degree of assurance that their system is protected against Trojans and other malicious software.

This is accomplished through an attribute called a security label. A security label is attached to every object and subject. When a subject desires access to an object, the system compares the associated security labels and if the subject's label dominates the

object's label, an access is allowed. The subject's security label is assigned when the user logs on to the system and is based on the security level of the session.

A military classification system provides a good example of how this process would work. User X has a SECRET security clearance and wishes to read a document that is labeled as TOP SECRET. He goes to the vault and asks the guard for access to the document. The guard checks the user's clearance and notes that he has a secret clearance. The guard enters the vault to retrieve the document. He checks the label on the document. Since it is marked as top secret, the guard leaves the document in the vault and tells the user that he is not cleared to access that document.

Implementing a mandatory access control policy ensures protection against unauthorized disclosure and unauthorized modification. Using the sensitivity labels allows for great flexibility in tailoring the mandatory policy to suit the individual needs of each organization.

Internally, the mechanism can be thought of as maintaining a table with three columns: subject, object, and access mode. This creates a mapping or matrix of authorized accesses and access modes. When a subject desires a certain mode of access to an object, the system examines this table and makes a determination if that subject is authorized to access the object in that mode.

The mandatory policy is persistent. This means that the entries in the table do not change, they remain constant. It cannot be said, for example, that Subject A is allowed Write access to Object X on a certain day of the week but not others. (This kind of rule falls into the category of discretionary access.) Since there is no middle ground, access control is either mandatory or discretionary, careful consideration of each rule must be made to determine if it truly is implementing a mandatory policy. By definition, a mandatory access control policy means that subjects cannot modify mandatory security authorizations [Brinkley].

One of the better known security models for MAC is the Bell and LaPadula model [McLean]. This model is concerned with preserving confidentiality. The two fundamental properties are: simple security and the *-property (pronounced star

property). In laymen's terms, the simple security property prohibits a lower sensitivity subject from reading a higher sensitivity object. The *-property prohibits a higher sensitivity subject from writing to a lower sensitivity object. When correctly implemented, this model provides mandatory access control for confidentiality.

Multiple mandatory policies may be used within a system. For instance, one set of security labels could implement confidentiality and another could implement integrity. For the purposes of this thesis, integrity labels will be omitted. Only those mandatory policies affecting confidentiality are considered.

7. Discretionary Access Control Policy

Discretionary access control allows the subjects in a computer system to decide who has access rights to their information. The access policy is at the subjects' discretion. This allows for a greater degree of dynamic control of access in the system. Object owners can decide who has a need and rights to access their objects for reading or writing. The owner can now exercise a great degree of control over his data.

Internally, the mechanism not only supports the subject, object, access mode table used in mandatory access control, but also allows for special rules such as allowing access only on weekends after 5pm.

While affording users greater control over their files, discretionary controls do nothing to prevent malicious software from stealing or damaging data. In fact, it may even help the spread of certain malicious processes. There is nothing to prevent a Trojan horse from granting access to files which the owner did not intend. Since the Trojan horse is executing on behalf of the user, it can do anything that the user could do. While discretionary controls may be useful, they are no substitute for a well planned and executed mandatory access control policy.

8. Assurance

An underlying theme in the previous paragraphs has been the notion of assurance. The assurance of a system refers to the amount of confidence that can be placed in the security mechanisms of that system. In other words, how much can the system be trusted? High assurance systems demonstrate through mathematical proofs and other techniques that the internal mechanisms completely implement the intended security policy.

One method originally advocated for gaining assurance in a system was a "penetrate and patch" approach. In this method, designers of a system would take on the role of attackers and try to introduce malicious software or exploit vulnerabilities and bugs in the system. If a security hole was discovered, the system software would then be corrected. The advantage to this testing is that many bugs in a system can be fixed before it is released to the consumer. Once this cycle of testing is completed, the designers would certify the system as secure with a high level of assurance.

The major flaw in this process, however, is that it is impossible for a single group of system designers to test for every possible flaw or contingency in the systems in question. The complexity of even simple systems is far beyond the ability to exhaustively test for all security holes. Even worse, many holes in a system are due to design problems, meaning that if the designers didn't catch the problem in initial design, they will more than likely overlook it when testing for vulnerabilities. And while testing may reveal some errors in a system, it cannot prove the non-existence of errors or subversion.

In light of the need for high assurance systems, the Department of Defense issued the Trusted Computer System Evaluation Criteria (TCSEC) in 1985 [NCSC]. This document states exactly what is required for systems to gain certification that they possess high assurance. The systems passing the given requirements would be given a rating ranging from (D) Minimal Protection to (A1) Verified Design.

Later, a need developed for an international standard for measuring the assurance of systems. Information security representatives from the U.S., Canada, France, Germany, and the U.K. created the Common Criteria Recognition Agreement (CCRA) [Cox]. The measures used in the Common Criteria gained international recognition and are used by most countries today. Systems are now rated with a set of Evaluation Assurance Levels (EALs). They range from EAL1 to EAL7 with each higher level providing greater assurance of correct policy enforcement.

9. Multilevel Network

A multilevel system provides a mechanism that allows for users with varying clearances to have controlled access to the resources contained on the system. The system protects information with a range of classifications. The system makes a determination based on the user's credentials about which resources he will be allowed to access.

Similarly, a multilevel network has network traffic of varying classification levels flowing over its wires. Security mechanisms restrict the flow of information among the networked objects. Because of this, users do not have to move among terminals or work areas to access their data at differing sensitivities. Instead, they can access their various sensitivity objects across a network connection using trusted clients. A multilevel network could then be comprised of single level and multilevel trusted machines.

Security, cost, and convenience may motivate the use of multilevel networks. It reduces the number of separate machines that individual users must log into and also reduces the operational costs of housing all of the extra equipment necessary to run separate networks for each classification level. Multilevel networks also allow the sharing of data across different sensitivity levels in real time.

The following is a real world example of a multilevel network in operation [NIST]. The command center at Barksdale Air Force Base had a need to allow its users access to up to sixteen different systems with varying sensitivities simultaneously. Of concern was the lack of physical space in the command center to house the machines necessary to accomplish this goal. A second concern was a reduction of operational costs. They were able to accomplish their goal using commercial-off-the-shelf products.

In this example, the leadership was focused simply on cost saving and not with any kind of security assurance. By using commercial products, only a low degree of assurance could be placed in this network.

The next chapter will present research questions of this thesis and look at the intended educational goals of the scenario developed for this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. SCENARIO GOALS

A. RESEARCH QUESTIONS

This thesis will answer the following question first: Can a scenario be developed that illustrates the concepts of Mandatory Access Control (MAC) and Discretionary Access Control (DAC) in a multilevel system? The scenario should address these issues as they relate to secrecy. The player will learn the effects that security-related choices he makes have on the ability to enforce MAC and DAC policies when assets need protection from unauthorized disclosure. This thesis focuses solely on the related concept of confidentiality policies and not integrity or availability. While integrity and availability are both important concepts to teach, coupled with confidentiality they are beyond an attainable scope for this scenario.

This thesis also answers a second question: Is it possible to validate that the CyberCIEGE game engine produces expected results from a specific scenario definition file and a prescribed set of player choices? This issue is addressed in Chapter IV.

B . SCENARIO EDUCATIONAL GOALS

1. Introduction

As was seen in Chapter I, there is a need for expanding the current methods employed to accomplish training in information assurance. The scenario written for this thesis will use the CyberCIEGE game as a tool for introducing and training the intended users in the areas described above in the first research question. The following sections will discuss the intended users of this scenario and the educational goals tailored to those users.

2. Intended Users

The intended users of the scenario are threefold. The first group consists of those network users who desire education in the security concepts presented in the scenario. The second group is comprised of the educators who are using the scenario as a teaching

tool and who may also desire to modify the scenario to meet their individual needs. The final group is senior leadership who is responsible for making security policy decisions in the organization.

a. Users Desiring Education

This first group is the primary audience of the scenario. These are the people in need of education in network security. This thesis assumes that Information Assurance students familiar with the DoD, particularly the military, are the users of the scenario. This group also contains some smaller subgroups. These subgroups include:

- Newly arrived personnel who have little or no initial training in computer security and require familiarization
- Transferred personnel from various career fields who may have some security awareness training or education
- Personnel requiring annual refresher training
- Computer and communication career field personnel desiring to continue their education
- Personnel in remedial situations requiring training in order to regain suspended network privileges
- Personnel in technical schools or in full-time student status

The beauty of the CyberCIEGE game is that it can be used in many different settings. Whether in a classroom situation with multiple players all working on various lessons, or individually as a continuing educational tool, the player needs only to load the scenario containing the relevant educational goals and he can begin to learn the associated concepts.

The objective is not to have the player simply memorize facts about security, but to actually learn them as concepts that can be applied in real world

situations. Once security becomes a learned behavior instead of a nuisance to be dealt with, the average user will incorporate stronger security practices into their routine network habits. Irvine and Thompson state that great benefits can be gained in computer security training and education with a simulation game by actually altering the behavior of users and policy makers [IRVINE].

b. Educators as Users

The second group using the scenario would be educators, especially those who teach Information Assurance curricula. They will have played and won the scenario themselves. The simulated game environment lends itself to playability in that a particular solution may work one time, and fail the next due to the random nature of the game, which will result in different types of attacks. For instance, in one scenario a player may successfully defend against an Internet hacking attempt, only to have his same solution fall victim to an insider attack the next time he plays it. The educator can now facilitate greater learning by using these various results as teaching illustrations. He may also use the game to assign lab exercises to reinforce the security topics under discussion in class. He can also point to the scenario as an indication of real world practices. Bad choices or habits may not always result in attacks or exploitation. This will cause the player to think through each decision and evaluate the impact on the overall security of the network.

There is enormous potential for teaching many security concepts even from a single scenario. The educator can decide beforehand which topics he would like to teach and have his students run the appropriate scenarios. If he is comfortable enough with the game, he may try his hand at editing or creating his own scenarios. He may also modify existing ones, changing various nuances in the scenario, to illustrate or emphasize selected concepts. The “save game” feature allows the teacher to play the scenario up to a certain point, or make certain network configuration choices, and then save the game. Thus the trainee student plays the game at the instructor-defined starting point.

c. Senior Leadership

The final group intended to use the scenario is senior leadership and policymakers. In the DoD, leaders at all levels are in just as much need of training as any

other users. These leaders set the example for their subordinates. They need to realize the necessity of following the rules set forth in their own security policies. Frustration can set in among the lower ranks in the face of double standards. For example, the security policy may prohibit the reading of Internet e-mail accounts from inside the organization's local area network. Average users may not regard the policy seriously if they see the general officers ignoring this rule and using their Internet e-mail at work.

When placed into the hands of these leaders, this scenario will promote a greater understanding of computer and network security. This will improve their ability to make coherent decisions and foster support for enforcement of the security policy at the highest levels.

This scenario is a tool to raise the awareness of senior managers and information security officers responsible for creating the organization's security policy. In doing so, these leaders should be able to make better, more coherent decisions regarding network security. This is especially important as reliance on technology to enforce the organization's mandatory policy continues to expand. Leadership needs to know the right questions to ask when considering new purchases or upgrades to current hardware and software.

Coupled with a dependence on technology is the risk of these technologies being subverted. Decision makers need to be aware of the manner that these subversions can manifest themselves and the precautions that can be taken to prevent them. The scenarios in CyberCIEGE can be a source of promoting this awareness.

There is educational potential for all three intended user groups. The players can learn security rather than memorize and forget. Educators have flexibility in determining the appropriate lessons a student should learn by selecting pre-written scenarios, or by manipulating a scenario to suit their particular needs. Higher ranking management can see first-hand the effects that their policymaking decisions will have on the security of the organization's network.

3. Educational Goals

a. Mandatory Access Controls

Mandatory access control is presented to the player in such a way that it can be learned and not just be a memorized definition. Current teaching methods involve memorization of definitions, classroom instructions, and lab exercises designed to emphasize the concepts. By introducing security in a gaming environment, the player gains an emotional investment in the security decisions. When used in conjunction with traditional training, this investment on the player's part will yield a deeper understanding and a better retention of these relevant security topics

There is an old story about learning to drive a car from reading a book. It is true that the potential driver can memorize what the gas and brake pedals are, and how to change gears. But doing these things does not mean he can actually drive. Driving takes practice. After becoming an experienced driver, most people do not even consciously think about pressing the gas and brake pedals or changing gears. Driving has become a habit and it is done without a second thought. In much the same manner, the player can practice at network security and learn good habits. These habits will then have a greater chance of becoming a part of that player's real world security practices.

The first educational goal is to teach the concept of mandatory access control. The scenario has a mandatory policy with several classification levels. Some of these are hierarchical in nature while others are non-hierarchical, or compartmental. The player must sort through the mandatory controls to determine which assets the security labels apply to and which users have the corresponding security clearance to access those assets.

The choices the player will make in the scenario revolve around the purchase of network components and their ensuing configuration to meet the users' asset goals. The player will have to place these components into some type of network configuration that will allow the mandatory security policy to be enforced while at the same time satisfying the productivity needs of the users. If the player makes poor choices, the game will respond by generating attacks that violate the intended MAC policies.

If the player opts to place all of his components on a single network, he will have to rely solely on high assurance components to prevent attacks. If he physically separates all of the networks and assets from each other, he will be unable to meet his users' asset goals. Only by using a combination of physical separation and high assurance multilevel components will he be able to successfully avoid attack. See Chapter 4 for greater detail on the testing of these player choices.

b. Discretionary Access Control

A second goal is to teach the player the effects his decisions have when attempting to implement a discretionary access control policy.

Each asset will have corresponding discretionary controls that the player will have to implement. Some users in the scenario will have motivation to attempt access to assets for which they are not the intended users. If these unauthorized accesses occur, the player will be penalized.

The scenario contains three discretionary groups. The Area91 group is comprised of all the personnel at the facility. All of the users are further divided into one of the remaining two groups – Scientists and Managers.

There are certain assets in the scenario belonging to the Scientists for which the Managers are not to be given access. Likewise, some assets belonging to the Managers are to be kept from the Scientists.

The player will have to assign all discretionary controls on the machines he purchases and places onto the network. The player could buy machines and satisfy his user goals, but improperly configure the discretionary access controls. As the game progresses, he will find that the machine is being accessed by unauthorized individuals. This will force the player to carefully examine each access control list. He may have to pay for better training for his users, or buy physical security devices as he attempts to solve the issue of how to properly implement the discretionary policies.

Each of the virtual users in the game will have a description of his position in the organization and his goals within the scenario. The player may examine these to determine the authorizations each user should have for each component. The player will

configure the access control lists on the components to enable the real-time sharing of assets among the users. Once everything is properly configured, the scenario will allow the player to progress and meet the needs of other users as funds become available.

c. Multilevel Network

The third educational goal is to teach the player good security practices in a multilevel network. The player will be presented with a facility completely empty of any physical network devices. He will have several users with varying clearances who require access to assets at different sensitivities. The player will have to buy all of the appropriate components and implement some type of security solution to meet the scenario goals. As the scenario progresses, the users within the game will have changing needs that the player will have to pay attention to in order to avoid penalties.

The player will be presented with the decision to buy components with varying degrees of assurance in the operating system's ability to enforce the MAC and DAC policies. Because of the cost of the high assurance machines, the player may opt to buy less trusted components. The confidentiality of the network would then be more likely to be broken because of this choice. The player will have to buy the high assurance machines in order to prevent unauthorized disclosure of the assets on the network.

The player will have to learn how to meet the needs of multiple users, some of which may conflict or even be unattainable. It is up to the player to sort through the goals of these users and prioritize them. He will have to make choices based on a limited budget which will not allow for all of the users' needs to be met initially. This should model the real world, in that an organization has finite resources and must strategically expend them to maximize their utilization.

This also ensures that the player must use good security practices. He will not be allowed to simply start the game on pause and buy everything he needs and then win. He will have to un-pause the game and let it run for at least several weeks of game time. This allows the game engine to generate any attacks based on incorrect security choices made by the player.

The player will win the scenario when he has met all of the user goals, and his organization does not disclose its high value assets for thirty days of game play. The player will fail if a highly classified secret is disclosed or some other attack causes his available funds to drop below zero dollars.

III. SCENARIO OUTLINE

A. OVERVIEW OF SCENARIO

This scenario has been designed to achieve the educational goals described in the previous chapter. This chapter describes the scenario and how it has been designed to meet these goals.

The scenario written for this thesis is set in a military type of installation on a fictional planet. Area 91 is the name given to this installation. It is located on Desmid, a world similar to Earth. Planet Desmid has a single world-wide government called the Planetary Council. This Council directly supervises all of the military activities of the planet, specifically those that occur at Area 91.

The player of the scenario will assume the role of the Computer Networks Officer for Area 91. The player is given a timeline in the game briefing that must be met in order to succeed in the game. An assumption made about the player is that he will take the time to read through the initial briefing, as well as the various user and asset goal descriptions, in order to become familiar with the requirements of the scenario.

The scenario begins with an initial welcome screen that directs the player to go to the game tab to see a full briefing. This initial briefing introduces the player to the Area 91 scenario. The briefing is intended to orient the player with the overall concept of the scenario, the types of assets he will be working with and protecting, an overview of the different groups of users within the scenario, and what the player must accomplish in order to succeed or fail. The briefing will also give some strategies and tips to the player to help him know where to get started. It points him to examine the needs of the users and their associated asset goals.

The following is the initial briefing:

Welcome to Area 91. This is Planet Desmid's premiere secret projects research facility. Please see the game tab for a full briefing.

Area 91 houses two major research projects. The first is code named Fender. The Fender project revolves around the production of a liquid-fluoride based mind control

serum. When introduced into the water supply, the surrounding population becomes highly susceptible to outside influences. The scientists at the facility have a formula for creating the serum, along with a database that tracks the various production batches of the serum. These assets are worth $1,000,000 to the organization and attackers have a very high motive for compromising everything Fender related. You can find more information about these Fender-related projects on the asset tab.

The second project is code named Nightingale. This project is concerned with the manufacture of tracking devices that can be implanted into humans. These devices are small biological microchips easily introduced into the human blood stream through an injection. The project team has the schematics for these biochips and a database of test results related to the experiments with the biochips. These assets are worth $500,000 to the organization and attackers are extremely motivated to disclose anything with this secrecy label. Look for more information on the asset tab.

Also look for details of other assets and the associated goals that the users in your facility have on the asset tab.

Area 91 has only recently been built and has no existing computer networks. Your mission as the Computer Networks Officer is to supervise the procurement and installation of the necessary components to allow the facility's users to do their work. There are two user groups co-located in your facility: scientists and managers. The scientists' goals revolve around accessing the various projects in the facility, while the managers' goals are to keep the facility running and to ensure that the projects stay on track. You can find more details about each user on the user tab.

You have been given initial funding by the Ruling Planetary Council of $1,000,000. You will also receive a monthly budget for your IT department of $2,000. If you use your funds wisely, the Council may give you more research grants later.

In order to win this scenario: you have to keep the facility going for thirty days without losing all of your money. If your balance falls below zero, you will lose.

Strategies and Tips:

On the user tab, each user has his asset goals listed along with their associated target usage amounts. You will notice as you progress through the scenario that some users have target usages of zero. This number will change as time goes by, so keep an eye on them.

Initially, only a few of your users have asset goals that need to be met immediately. Concentrate your efforts on meeting the needs of those users who are involved with creating the daily situational report. This daily report keeps the Planetary Council apprised of the progress of the projects at Area 91.

After 5 days, users with goals to access Internet Research and Scientific Research Databases will change. Also, note that the needs of the users responsible for the daily report may change as well, so be sure to check everyone's goals on the fifth day.

After 10 days, the asset goals of the Nightingale project team will change. They will need to be provided with the necessary resources to access their assets. Look for details on the user and asset tabs.

On day 15, your Fender project team will have goals that will need to be met.

Also, for further help, you may press 'e' to bring up the game encyclopedia.

If the player skips the briefing and proceeds to play the game, he will miss several important aspects of the scenario. The first thing he will miss is the changing user needs as the scenario progresses. Since this thesis assumes the player is familiar with the game interface, the player may make the mistake of trying to meet all of the users' goals and then unpause the game and let it run. At day five, some of the users' goals change and the player may not be aware of it and start to experience unexpected productivity losses. This will be repeated on days 10 and 15 as well.

The second area that the player will miss is the strategies and tips section. The player could spend all of his money on certain items that are not necessary for this

scenario. The strategies and tips section is designed as a starting point for the player. Although it is not intended to give the solution, it is supposed to point the player in the general direction of a positive solution.

B. ASSETS

Once the player has read the initial briefing, he may click on the asset tab in order to familiarize himself with the various assets in the game that need protecting. Some of these assets are more valuable than others, and, if compromised, more damage would result for the organization than for other assets. The story line of the scenario involves the player making choices on how best to maintain the confidentiality of these assets. These choices will illustrate the MAC concepts described in the educational goals.

There are two code named asset groups in the scenario, Fender and Nightingale. These are the highest sensitivity labeled assets in the organization. The mandatory policy describes a hierarchical security scheme with Fender and Nightingale being non-hierarchical compartments at the highest level. The remaining sensitivity labels, in order from most sensitive to least, are Secret, Sensitive, and Unclassified. None of these labels has a non-hierarchical component. Due to the sensitive nature of the Fender and Nightingale assets, attackers have the highest motive to violate their confidentiality and availability.

The Fender assets revolve around the Mind Control Formula; and the Nightingale assets are related to the Biochips. These two compartmented types of assets are the most valuable in the scenario and will cause the most damage to the organization if disclosed. These assets are intended to illustrate to the player how to configure network security so that the users with these clearances can have access to their assets and all other assets dominated by their security labels, but not the assets in the other compartment. When the player purchases components in the scenario, he can set the minimum and maximum intended security labels for the assets contained on those machines. For instance, the player could select “Unclassified” as a minimum and “Fender” as a maximum. He could not, however, set “Fender” as a minimum and “Nightingale” as a maximum because Nightingale’s security label does not dominate the Fender security label.

The player is prompted by the briefing to look at the Daily Report first. This report is generated for the Desmid Planetary Council and is used as a means of situational reporting up the chain of command. All network control centers have some type of reporting that must be accomplished. Whether military or civilian, senior leadership needs to be kept apprised of the current health of the network.

In this scenario, the "Managers" user group is responsible for modifying this report. A tension introduced with this asset is the fact that the managers wish to keep the "Scientists" user group from gaining read access. The managers know that the ongoing funding from the Council depends on favorable progress reports from Area 91. The report often blames the scientists for any setbacks or failures. The scientists at the facility would be disturbed to find themselves portrayed in a negative manner.

Conversely, the scientists also have their own secrets that they don't wish the managers to discover. The Liquid Fluoride Production Database shows that the Mind Control Formula doesn't actually work; and the Human Biochip Implant Test Data shows that the project has fallen far behind its projected schedule.

These two conflicts are designed to force the player to implement some sort of discretionary controls on the assets. Even though internal disclosure of these assets will not cause the game to fail immediately, it will serve as a source of disruption and could cause enough of a loss in productivity that the player has insufficient funds to finish the scenario.

The following is a listing of all of the assets in the scenario with their corresponding descriptions:

Liquid Fluoride Mind Control Formula*: The scientists at Area 91 have a formula for producing a liquid fluoride-based mind control serum. They have code named any research related to this formula as Fender. All Fender assets are the most valuable possessed by this organization. When placed into the water supply, it reduces the ability to make decisions, making the surrounding population more docile and easier to control. This formula consists of the mathematical models and detailed chemical properties of the formula. If this formula falls into enemy hands, the results would be*

catastrophic. Enemy scientists could formulate ways of detecting the presence of the liquid, or could formulate antidotes. Also, the formula could be quickly used as a weapon against us, causing our demise. Only users cleared to Fender should have access to this data.

***Liquid Fluoride Production Database**: This asset contains an inventory of every batch of mind control serum produced at Area 91. It also lists each corresponding production serial number, storage location, and/or release site for each batch of serum. While the military leaders consider this project to be their greatest accomplishment, the scientists have run into a snag. After years of testing, they have concluded that the formula doesn't actually work. Since this database reflects the failure of this formula, the scientists would prefer not to allow project management access. There will be $10,000 in costs related to disruption should an access violation occur; and management has a fairly high motive to read this database.*

***Human Biochip Implant Schematics**: The designs for a computer chip that can be placed into humans for tracking purposes are the next most valuable asset held by the military on this planet. These chips are usually implanted into unsuspecting civilians during routine vaccinations at local doctor's offices. The military uses a super-computer to catalog and track the movements of the entire population. If the schematics were to become known, our enemies would possess the ability to mask or spoof the signals coming from the biochips. Also, they could track the population themselves, as well as produce their own implants. This research has been code named Nightingale and only users with this clearance should have access to this data.*

***Human Biochip Implant Test Data**: This asset consists of the latest test results for the working version of the biochip designs. It is based on a modeling program that uses the Biochip Schematics. Since this database reflects how far behind the Nightingale project is, the scientists would prefer to keep it from the Planetary Council which means keeping it out of the daily report. If this information is leaked to the Council's informants, it will cost the enterprise $5,000 in disruption and the informants have a motive to access this information should the opportunity present itself.*

***Daily Report**: This report is prepared for Planet Desmid's Ruling Planetary Council to keep it aware of the daily ongoing operations at Area 91. The facility's funding for its projects depends completely on favorable progress reports to the Council. Since these reports blame program slip-ups on the scientists and glosses over management's role in any blunders, morale among the scientists would be totally jeopardized if these reports are disclosed to them. This would cause $3,000 worth of damage to Area 91's funds and the scientists have a higher than average motive to read these reports.*

***Daily Report Checklist**: This checklist contains the necessary steps to create the daily report. The Ruling Council is extremely particular about the content and format of the daily report. This checklist must be followed exactly or the daily report will be rejected by the council and funding for the facility will be suspended.*

***Scientific Research Database**: Some of the scientists are not cleared to the code name projects but nonetheless are able to conduct research indirectly related to the projects. This database represents the ongoing research conducted by these scientists with only a Secret clearance. The Fender and Nightingale users assign research topics related to their work and will need access to the database to track the ongoing progress of these topics.*

***Administrative Files**: Check the user tab to learn which of the managers is responsible for the day-to-day operations at the facility. This asset represents the personnel records, interoffice memorandums, service contracts, and other administrative data required to keep the facility operational. Without this repository of files, the facility would cease operations resulting in a total shut-down.*

***Internet Research**: Posing one of your greatest security risks is your connection to the Internet. New users assigned to your facility are given the responsibility of conducting open source research, pending verification of their security clearance. You begin with a router in one of your zones with an Internet connection to an offsite machine containing this asset. The challenge will be to keep data from flowing out of your facility.*

Improper security configurations could allow outsiders access to confidential data on your network. Be careful what machines you allow to be connected to this asset.

***Work E-Mail**: All of your users would like to be able to read and write e-mail. Communication between the members of the various project teams is vital for productivity and the morale of the users. Providing all users access to this asset will have the greatest impact on the happiness of your people.*

C. ASSET GOALS

On the asset tab in the game, the player will also be able to read about the various asset goals in the game. The simulation engine for the game is still under development (21 April 2004) and only permits the player to see the descriptions of the first eight asset goals. It is expected that this number will be increased prior to the first official release of the game. The player can still see all of a user's goals on the "User" screen. While this screen does not list the descriptions of the asset goals, a separate document containing the descriptions could be given to the player which represents a workaround until the limitation on listed asset goals is fixed.

There are thirteen asset goals in this scenario. Each asset goal describes a user's desire to have some form of access to an asset in order to accomplish his mission. Typically these goals are either "read" or "read and write" (modify) access. The description for these asset goals states explicitly the access mode and the asset name.

The challenge for the player is to match these goals with the corresponding user who has that goal. More than one player may have the same goal. For instance, a goal may be to read and write e-mail. More than one user has this goal. The player must decide how to give access to the same asset to several users.

Another challenge is that of shared goals. These goals involve the concurrent access of an asset by more than one user. In this type of shared goal, all of the users with that goal must be able to access their asset simultaneously or all will fail. An example of this is the Daily Report asset. Several users have a shared goal to modify the Daily Report. If even one of the users with this goal is unable to modify the report, the report is

of no use and none of the users achieve that goal. The idea behind this is that the users with this goal have varying clearances with machines on separate networks. The player must decide how to grant simultaneous access to the Daily Report while preserving the integrity of the network security architecture.

Added to the necessity of shared goals, many users also require access to assets at varying sensitivities. The player will have to implement some form of multilevel network in order to accomplish these goals. For instance, Patrick (see users in section IV), has asset goals at the Fender, Secret, and Sensitive secrecy labels. The player could simply purchase a multilevel machine and place all of the assets he needs directly on the component. Other users, such as Jonathan, will also require access to the assets at these varying levels. The player will have to configure some type of network solution that allows multilevel access to the various assets. This will serve to meet the educational goals related to teaching players about multilevel networking.

The player is also presented with the challenge of a limited budget to meet his goals. Initially, the player is given just enough funding to satisfy the initial set of user needs. As the scenario progresses, he will be given more funding. How the player spends his money will greatly impact his ability to finish and win the scenario.

Finally, the player must face the changing needs of his users. This models the real world in that research projects come and go over time. Research grants are typically given with an associated timeline. As the player unpauses the game clock, the needs of the facility's users will change. The player must watch these needs to ensure that the virtual users remain productive.

The following are the descriptions of the asset goals in the scenario:

Modify Mind Control Formula*: This goal requires modification of the Liquid Fluoride Mind Control Formula. As the scientists continue to experiment with the formula, they will need to change the mathematical models and chemical properties stored in the formula. This goal will require the use of a word processor application.*

***Read Mind Control Formula**: This goal requires read access to the Liquid Fluoride Mind Control Formula. Some of the scientists who are responsible for working on the liquid fluoride production database will need read access to this asset in order to properly track changes made in the formula and update the database accordingly. This goal will require the use of a word processor application.*

***Read and Write Work E-Mail**: This goal requires read and write access to the Work E-Mail asset. Note that this asset is labeled as sensitive and that all of the users have this goal. The scientists and managers at the facility are dependent upon e-mail access to communicate between each other. If users fail this goal, their happiness will be greatly diminished. This goal will require the use of an e-mail client.*

***Modify Fluoride Database**: This goal requires modification of the Liquid Fluoride Mind Control Database. The scientists who use this database will also require read access to Liquid Fluoride Mind Control Formula.*

***Read Fluoride Database**: This goal requires read access to the Liquid Fluoride Mind Control Database. The scientists responsible for modification of the formula would like to keep track of the changes made to this database.*

***Read Research Database**: This goal requires read access to the Scientific Research Database. Each of the code word scientists has various research projects they have handed down to the scientists only cleared for secret work. These lower cleared researchers modify the Scientific Research Database and the code word scientists require read access to track the progress of their projects.*

***Read Internet Research**: This goal requires read access to the Internet Research asset. The scientists who possess a clearance would like to keep track of the current progress of the Research being conducted at the unclassified level.*

***Modify Internet Research**: This goal requires modification of the Internet Research asset. Failure to meet this goal will result in an almost total loss of productivity of the unclassified users. This is a collaborative effort that will fail unless all users who have this goal are able to modify this asset.*

Modify Biochip Schematics*: This goal requires modification of the Human Biochip Implant Schematics assets. As work progresses on the biochips, the scientists responsible for this project will need to update the schematics to reflect the current working version of the biochip.*

Read Biochip Schematics: *This goal requires read access to the Human Biochip Implant Schematics asset. The scientists who track testing results on the biochips will need to be able to read the current schematics so that they may make correct entries into the test results database. Users with this goal will require a word processor application.*

Modify Biochip Test Results*: This goal requires modification of the Human Biochip Implant Test Data. This test data is used in the ongoing experimentation with the biochips. Each new chip design is tested for human compatibility or rejection, transmitter strength, battery life, and adverse health risks in the human subjects. Several humans have been abducted from the planet Earth to accomplish these tests. Users will need a spreadsheet program to accomplish this goal.*

Read Biochip Test Results*: This goal requires read access to the Human Biochip Implant Test Data. The current working version of the biochips is completely dependent upon the interpretation of previous test experiments on the abducted humans. This goal will also require a spreadsheet application in order to succeed.*

Modify Daily Report*: This goal requires modification of the Daily Report asset.*

D. USERS

The scenario introduces the tension of untrusted users who need access to the facility in order to accomplish their goals against a set of trusted users and assets that must be protected. The player must make choices on how to best give them access to their assets while maintaining the security of the network. The Fender and Nightingale cleared users start the scenario with high background checks and high levels of trustworthiness. The Unclassified users have no background checks, and lower levels of trustworthiness. Raising the trustworthiness of these users by buying higher background checks will be cost prohibitive to the player. The scenario only gives the player enough

money initially to buy the components and physical security settings necessary to meet the users' goals. So the player will have to face the dilemma of meeting these untrusted users' needs without buying higher background checks.

The strategy for user clearances is straightforward. The more sensitive the clearance needed by the user, the higher his initial background check. Unclassified users have no background checks, Sensitive users have Low background checks, Secret users have Medium background checks, and the code word-cleared users have high background checks. None of the DAC groups is assigned an initial background check.

Once the player has read the initial briefing, he may press the user tab to learn more about the users in the scenario. Each user has his own set of asset goals he wishes to accomplish. Some users start with no immediate needs, but as the scenario progresses, these will change. As the player makes changes in the scenario, he will refer back to the user tab constantly to check on the status of the users. Each user has several items listed that the player needs to pay attention to.

First is a description of the user. This section is designed to give the player an overview of the user and his needs. It tells the player how that user fits into the scenario and any tensions introduced by having this user in the facility. For instance, the player may be told that the user is not trustworthy. This would provide a clue that the user should be closely monitored as to which zones and assets he has physical access to and what his background check level is.

The User tab also lists which DAC groups that the user belongs in. There are three groups defined in the scenario and a fourth built into the game engine. The groups are Area91, Managers, and Scientists. The Area91 group is analogous to the Everyone group in the Windows 2000 operating system. All of the users in the facility belong to this group. All of the users are then divided into the two remaining groups: Scientists and Managers. The fourth, built in group is called "PUBLIC". This represents the outside world, a source of many types of attacks on network security.

The intrigue built into the scenario highlights the security considerations of a DAC policy independent of the mandatory policy. The player must watch the Scientists

and Managers groups, as each one has motivation to violate the discretionary access control policies and see the other group's assets. In dealing with keeping these groups from accessing the other group's assets, the player will learn the concepts associated with the educational goals related to DAC.

Also contained on the user tab screen is a listing of asset goals associated with each user. When a player selects a user on this screen, he will see all of that user's goals and the target usages of that goal. The target usage represents a percentage amount of the user's time that he wishes to use to access that asset. For instance, a target usage of 25% means that the user wishes to access that asset 25% of his time. The sum of the target usages for all of the asset goals of a single user should not exceed 100%.

If the currently selected user has any asset goal failures, these will be listed on the screen as well. The player will spend much of his time on this screen. As he makes changes to the network, he will refer back to this section to determine if these changes have allowed the currently selected user to reach his asset goals.

The following is a description of each of the users in the scenario:

Patrick: *Patrick is the inventor of the Liquid Fluoride Mind Control formula and the chief scientist on the Fender project. As the project chief, he is responsible for modification of the formula as research progresses and advancements are made. He also needs to keep tabs on the Fluoride Production Database to ensure correct entries are being made by his assistant, Hector. Patrick also hands out assignments to Jessica, and needs to track her work by having read access to the Scientific Research Database. Patrick would prefer to also have access to the Internet Research if possible. Finally, in order to communicate with Hector and Jessica, as well as the facility management, he needs access to e-mail.*

Hector: *Hector is Patrick's lab assistant and is in charge of updating the Fluoride Production Database as new batches of the serum are produced. Hector catalogues each batch of serum and tags them for tracking purposes. Patrick allows Hector to follow his work on the formula, so he will require read access to that asset.*

Hector also monitors the Scientific Research Database for any breakthroughs and would also like to access the Internet Research asset. Hector also requires the ability to read and write e-mail.

Jonathan: *Jonathan is the lead scientist on the Nightingale project. The Desmid Intelligence Agency delivered the Biochip plans to Jonathan for safekeeping and further research. He may be a bit unscrupulous at times, prone to take shortcuts, and sloppy in his work. He only maintains his position as project leader due to his connections with the Agency. Jonathan's goals are to gather as much information from the various projects in the facility as possible. This includes the Scientific Research Database, even though Patrick is responsible for giving Jessica her work, Jonathan is motivated to try to "sneak a peak" at the work being done. Jonathan needs to read the latest Biochip Test Results and the Internet Research. In order to communicate with his team, give him access to read and write e-mail.*

Ivan: *Ivan coordinates all testing and research on the current working version of the biochips. He reads the current schematic, performs his tests and then takes the test results and inputs them into a spreadsheet for correlation and comparison analysis with previous versions of the chip design. Ivan also conducts some research at the Secret level and stores these in the Scientific Research Database. He also requires access to the Internet Research and the ability to compose e-mail.*

Brent: *Brent is one of two managers responsible for reporting on the code named projects to the Planetary Council. Brent's area of expertise is the mind control formula. His position as a senior manager dictates that he must have access to the formula and any research being conducted at the Secret level or below. Brent needs to be able to modify the Daily Report simultaneously with Michael and Janet. He also requires the ability to compose e-mail.*

Michael: *Michael is the other senior manager, along with Brent, who is responsible for reporting on the code named projects to the Planetary Council. Michael has been given a Nightingale clearance for the purposes of reporting on the status of the biochip research. As such, he requires read access to the current version of the Biochip*

Schematics. He needs to modify the Daily Report simultaneously with Brent and Janet. Since Brent handles reporting on the Secret and below projects, the only other goal for Michael is to read and write his e-mail.

Jessica: *Jessica is a younger scientist who works for Patrick. He gives her research projects and she tracks her progress on these in the Scientific Research Database. She keeps Patrick informed of her progress by sending coded messages via e-mail.*

Mary: *Mary's main responsibility is to conduct open source research on the Internet. She is handed various topics by Patrick and Jonathan and uses these as a basis for her work. Due to the large number of topics in her current workload, she has been assigned an assistant to split the load. As a result, she and Peter must collaborate together to modify the Internet Research database. She is given her topics through the e-mail system.*

Janet: *Janet is the senior editor of the Daily Report. The Planetary Council is extremely conscientious of the formatting and appearance of the report and has given Janet a Checklist to ensure that the report matches their specifications. While Janet shares the responsibility of modifying the report with Brent and Michael, she ultimately ensures that the report makes its way up the chain of command. She also keeps tabs on the Administrative Files to ensure that Greg is fulfilling his requirements as the facility administrative supervisor.*

Greg: *Greg is the facility's administrative supervisor. He keeps the facility operating from day to day. He handles all contracts with service providers and all human resource issues such as personnel and finance. He stores all information related to these activities in the Administrative Files asset. He also is responsible for dispensing any bulk e-mails to the facility's users.*

Peter: *Peter works closely with Mary to conduct research on the Internet. He has been brought in solely as a means to ease Mary's workload and possesses no security*

clearance. He has basically been given a desk in a corner and told to stay there while in the facility. He is curious about what goes on the facility and may get caught wandering around from time to time.

E. CONCLUSION

Each user should present a unique obstacle to network security that the player must overcome. By dealing with untrusted users in a high assurance facility, the player will learn the concepts of mandatory access and physical security. The tensions among the user groups illustrate the educational goals of discretionary access. And by forcing the player to provide access to assets at various sensitivities, the security issues involved with multilevel networks will be learned.

The next chapter will discuss the proposed solution to the scenario and the testing done to verify the game engine responds in a manner expected given certain conditions in the scenario definition file.

IV. TEST PLAN

A. TESTING PROCEDURE

1. Overview

This chapter examines the research question: Is it possible to validate that the CyberCIEGE game engine produces expected results from a specific scenario definition file? This chapter discusses the methodology employed to test the game engine. It will then explore three proposed solutions for the scenario written for this thesis. Next, it will compare the proposed solutions with the expected results and compare them to actual game play results. And finally, this chapter will explore the smaller scenarios written to test specific aspects of the game engine.

2. Methodology

The approach taken for testing expected game results from the CyberCIEGE game engine was twofold. First was the testing done using the full Area 91 scenario. Coupled with this was the simultaneous development of smaller scenarios used to test specific aspects of the game as they related to game play issues in the Area 91 scenario.

The solutions to the Area 91 scenario were developed in conjunction with the writing of the scenario. Using these solutions, a set of expected results from the game was written. The game was then played using only the solution as a blue print for actions to take in the play of the game. The actual game play results were then compared to the expected results to verify that the game responded as expected.

The smaller scenarios written to test specific aspects of the game will be discussed in section five. The next few sections deal solely with the results of the full Area 91 scenario.

The solutions examine three possible methods for playing the Area 91 scenario. The first solution makes all choices in the game using only a single network. All servers and workstations will be placed on the same network relying completely on low assurance components for the enforcement of MAC and DAC to prevent any security breaches. The second solution utilizes separate networks for each of the security labels. Each of the security classes will be placed on its own separate network, relying on

physical separation to prevent unauthorized disclosure of assets. The third solution implements a multilevel network with high assurance components. This solution relies on a combination of physical security and MAC policy enforcement by the operating systems on the high assurance components.

B. PROPOSED SOLUTIONS

1. Single Network Solution

This solution outlines the steps necessary to complete the scenario using only a single network for all of the components and low assurance machines. The player may make the assumption that he can place all of the components with their corresponding assets on the same network, and may be unwilling to pay the extra price necessary for higher assurance machines. In this situation, the highly valued assets such as the Mind Control Formula will be residing on the same network as the sensitive and unclassified assets. This means that the less trustworthy users will have potential access to the higher cleared assets.

This solution illustrates that the MAC policy enforcement mechanisms are vital to maintaining the confidentiality of the organization's assets. If the player does not purchase high assurance components, less trustworthy users will disclose the assets.

The proposed solution makes all changes to the zone physical security settings as well as default component procedural settings for components placed into the zones. These changes are done before any components are purchased. After clicking on the Zone tab, some areas to look at are access lists to the various zones, physical security settings, and minimum and maximum secrecy labels. The solution also requires hiring of security guards and IT staff.

This solution places all of the purchased components onto the SLAN network. It also accounts for purchasing background checks and user training for those users who require these upgrades. The exact list of steps for this solution is listed in Appendix A.

2. Separate Networks Solution

This solution illustrates another approach that the player may take when playing the scenario. In this version of the solution, the player physically separates all of the assets onto separate networks according to their security class. The Nightingale assets will only be allowed on the NLAN network, the Fender assets will only be allowed on the FLAN network, and so on.

This should prevent all disclosures of the high value assets, as only the most trusted personnel will be allowed physical access to the highest valued assets; and there are no possible information flows across networks.

See Appendix A for the exact list of steps required for this solution.

3. Multi-level Network Solution

This solution represents an answer to problems presented by the previous solutions. In the first solution, all users are able to meet their goals, and the network configuration is easier and cheaper, but it does not provide adequate security to protect the confidentiality of the assets. The second solution provides much higher security, but at the expense of productivity losses and failed user goals.

By purchasing high assurance components, users can maintain productivity by accessing assets at varying classification levels while maintaining a high degree of protection from confidentiality breaches.

See Appendix A for the exact list of steps required for this solution.

C. COMPARISON OF EXPECTED RESULTS TO GAME PLAY RESULTS

1. Single Network Solution

a. Expected Results

The implementation of a single network with assets at all classification levels residing on it should result in three main types of attacks. The first expected type would be external hacking attacks. This is due to the presence of an Internet connection directly on the only network and assets present on that network that are highly attractive to hackers. The second type of expected attack is an insider-motivated public disclosure of assets. This is due to the fact that users with little or no background checks and varying

degrees of trustworthiness have physical access to the network and thus an avenue for reaching the high value assets. The final expected type of attack would be denial of service attacks. Since there is only one network, and that network contains the assets with the highest denial of service motives, the entire productivity of the facility would be destroyed by a single attack of this type.

b. Actual Results

Refining and testing the proposed solutions and results was not accomplished due to the unavailability of a stable game engine during thesis development. Several of the smaller scenarios written in support of the full scenario have test results which are applicable to this case. These are described in Section D below. In particular, the test case involving three users in a single zone did show that untrusted users will disclose high value assets when allowed physical access.

2. Separate Networks Solution

a. Expected Results

This solution attempts to mitigate the vulnerabilities from the first solution. By physically separating the assets based on their security labels onto different networks, the flaws of the single network solution should be avoided. The external hacker could only get, at most, access to the single network connected to the Internet. Since this network only contains the Internet Research asset, this poses absolutely no threat because the asset represents information that is freely available from open sources. By having good physical security and zone access lists, only the most trusted users with the highest background checks would be allowed access to the highest valued assets. This may not completely remove the threat posed by an extremely determined insider, but this does model the real world. Finally, a denial of service attack could potentially occur, but since each network is isolated from the others, the greatest threat is the loss of productivity from a single network while the rest of the organization remains unaffected.

While this solution does eliminate a great deal of risk, productivity is sharply affected. The users in the scenario cannot get to all of the assets they need from a single machine. They must spend their time wandering from zone to zone. This greatly hampers productivity and dampens the morale of the users.

b. Actual Results

Refining and testing the proposed solutions and results was not accomplished due to the unavailability of a stable game engine during thesis development. A smaller scenario with features similar to this solution is described in Section D below. The three users in two zones scenario represents the physical separation of an untrusted user from a high value asset. In this case, disclosure of the high value assets was prevented. This case did not consider any productivity losses associated with physical separation.

3. Multi-level Networks Solution

a. Expected Results

This solution accepts the fact that a standoff between security and productivity has occurred. Putting all of the organization's assets on a single network is an unacceptable security risk and having extremely high physical security incapacitates productivity. What is needed is a way for users to access their assets without sacrificing security.

The proposed method in this solution is the introduction of high assurance multilevel systems. These systems are designed with mechanisms built into their operating systems that prevent unintended information flow between assets of different classifications. These systems can then be placed on two or more networks allowing the user simultaneous access to assets at varying classification levels. While these machines physically are connected to multiple networks, logically it is as if each of the networks is separated from the other.

The expectation is that productivity will be greatly improved from the second solution while at the same time the attacks experienced in the first solution would be avoided.

b. Actual Results

While testing and refining of the proposed solutions was not accomplished, the results from testing a smaller scenario can be pointed to as an indicator of the actual results of implementing this solution. The four users in two zones scenario described in Section D shows that it is possible to utilize a high assurance operating

system and prevent disclosure of assets by an untrusted user. The multilevel architecture solution would be implemented with these high assurance machines.

D. SMALLER SCENARIO TESTS

1. Shared Goal Scenario

This scenario was written to test the sharing aspect of an asset goal. In the Scenario Format Template an asset goal has a Boolean field called “shared”. If this is set to true, then any users with this goal must all be able to simultaneously attain that goal or all such users will fail. This is a model of the real world concept of project collaboration.

This scenario has two users, Patrick and George. They have a shared goal of modifying the Liquid Fluoride Mind Control asset.

During game play, the users were each provided with workstations. The asset was placed onto Patrick’s machine. Checking the user tab at this point revealed that both users still had an asset failure. The two machines were then placed onto the FLAN network and George was given remote access permission to Patrick’s computer.

The result when checking the user tab at this point was that neither user had asset failures. The sharing aspect worked as expected.

See Appendix C for details of this scenario.

2. Three Users in One Zone Scenario

This scenario was written to test the results of having an untrusted and uncleared user in a zone with high value assets. Is it possible to have high assurance components and prevent this user from accessing the assets?

This scenario builds on the shared goal scenario. A third user, Howie, is introduced. The Fender secrecy label is set to an attacker value of 600. The attacker value is a scale from 0 to 999. Zero represents the fact that attackers would have no motive to access an asset with this security label and 999 is the maximum motive.

The game was first played using ordinary Blato desktops to hold the Liquid Fluoride Mind Control asset. Howie almost immediately disclosed the asset. Physical security was then increased to the maximum possible to see if Howie could be deterred, but he still disclosed the asset.

The attacker motive was lowered to 300 with the same results. The scenario was run using Trusted Targo Worksavers, the equivalent of a Windows NT operating system. The results did not change.

The conclusion is that no amount of physical security is going to stop a highly motivated insider from disclosing assets on low assurance components to which the user has physical access.

The scenario was played for a third time using high assurance components equivalent to EAL7 and an attacker motive of 600. Even with high assurance components, Howie still could not be deterred from disclosing the Liquid Fluoride Mind Control Formula asset. Preventing Howie physical access to the high value asset seems to be the only means of maintaining confidentiality.

See Appendix C for details of this scenario.

3. Three Users in Two Zones Scenario

This scenario was written to test the hypothesis that putting an untrusted user in a separate zone and denying him physical access to a high value asset will prevent its disclosure. Physical security should be able to prevent an unauthorized user from entering a restricted area and thus keep the assets guarded.

The three users in one zone scenario was expanded to include a second zone. In this version, Howie is only allowed access to a zone with a low attacker value security label. The highly valued asset, the Mind Control Formula, is placed in the Fender zone.

With an attacker motive of 600, Howie never disclosed the formula. The lesson here is that good physical security practices play an integral part in network security.

See Appendix C for details of this scenario.

4. Four Users in Two Zones Scenario

This scenario was designed to test the idea that a high assurance component should be able to prevent an unauthorized user from gaining access to a high value asset.

A fourth user, Stanley, is introduced into the three users in two zones scenario. He is cleared to Secret which has an attacker motive of 300. He is given a machine running the Secure Shade Desktop operating system with a Secret asset called Research Database. This machine is placed in the same zone with Howie. The high assurance OS still does not keep Howie from disclosing the asset.

The scenario is run again, this time using the Green Shade Core high assurance operating system. In this scenario, Howie did not disclose the Research Database. In this case, one high assurance operating system, Green Shade Core, was able to prevent disclosure while the other, Secure Shade, was not.

The conclusion reached is that the highest assurance machines can make a difference when attempting to thwart the attacks of insiders with relatively high motivation.

See Appendix C for details of this scenario.

5. Asset Usage Change Scenario

This scenario was written to explore a problem encountered with the game engine. The full Area 91 scenario relies heavily on the concept of the changing asset goals of the users in the facility. The initial concept was to give users new asset goals as time progresses in the game.

The first iteration of this scenario started with a single user with no asset goals. On the second day, a change asset usage trigger was written to add an asset goal to the user. Unfortunately, the trigger went off, but the asset goal was never added. The conclusion from this exercise is that for a user to be assigned an asset goal, he must start

the scenario with the goal already defined for him in the SDF. It cannot be given to him dynamically through the use of a trigger.

This brought about the next evolution of the scenario. The user was given a zero target usage as an initial asset goal. The idea being that the trigger would then change the target usage to 100. Since the user was given an initial target usage of zero, which means that he wants to spend zero percent of his time meeting this asset goal, he should have no asset goal failures.

When this scenario was run, it was discovered that even with a zero target usage amount, the game still listed the user as having an asset goal failure and penalized productivity accordingly. As a result of this penalization, the change asset usage trigger became practically useless and the full scenario could not be implemented as initially planned.

This test case resulted in a modification to the game engine. Testing this fixed version of the game was not accomplished as part of the work reported here.

See Appendix C for details of this scenario.

6. Cash Change Scenario

This scenario was written to test the game's ability to adjust the amount of cash on hand. In the full Area 91 scenario, at five day intervals the cash is increased to represent research grants being given to the scientists at the facility.

In this small scenario, an adjustment to the cash on hand is made on the second day through the use of a cash change trigger. When the scenario was run, the trigger worked exactly as expected.

See Appendix C for details of this scenario.

7. Two Lose Triggers Scenario

This scenario was written to test the game's ability to support more than one trigger of the same type. In this case, the trigger tested was a lose trigger. Having several triggers of the same type was crucial to the writing of the Area 91 scenario. In earlier

testing of the Area 91 scenario, the game engine seemed to ignore some of the triggers. This smaller scenario was written to determine whether there was a problem in the game.

In this scenario, there are two lose triggers. One is set to go off on the second day, the other is set to go off of when the cash on hand falls below zero. To test the first trigger, the game was unpaused and allowed to run for two days. At day two, the lose trigger fired. To test the second trigger, the surveillance cameras on the zone tab were purchased to cause the cash to go negative. As soon as the game was unpaused, the second lose trigger fired.

Upon running this scenario at various speeds within the game, it was discovered that the game engine sometimes skips triggers. While running the game, it is possible to speed up the game clock by two, four, eight, sixteen, or thirty-two times normal. The game consistently skipped triggers when running at 32 times normal speed. Based on these results, all test cases performed after this used at most the sixteen times normal speed setting. Note that the 32 times speed is intended for debugging purposes and not actual game play and does not represent a failure of the game engine.

See Appendix C for details of this scenario.

8. Two Triggers At Once Scenario

This scenario was written to test the game's ability to have multiple triggers execute off of the same conditions. This was important to the Area 91 scenario because many of the triggers depended on the same condition. For instance, on the fifth day, several triggers change users' target asset goal usage amounts.

This scenario tests the ability to have a message and a log trigger execute from the same time condition. The condition used was a time condition set to become true after 24 hours. When the scenario was run, both triggers fired exactly as expected.

See Appendix C for details of this scenario.

9. Inheritance Check Scenarios

This series of scenarios was written to verify that the default component procedural settings were being inherited by newly purchased components placed into that zone. A simple baseline scenario file was written. While the scenario was being run, each of the default procedural security settings was examined individually. For each one, the setting condition would be set on the zone tab screen, a new component would be purchased, and then the component would be selected on the component tab. The procedural security setting being examined would then be compared to the setting just changed on the zone tab. If they matched, then the test passed, if they did not match, the test failed.

Table 1 summarizes the results of the inheritance checks:

Filename:	Tests Change Setting to:	Results:
Inheritance Check 1	Password Length Medium	Passed
Inheritance Check 2	Password Length Long	Passed
Inheritance Check 3	Password Character Set Moderate	Passed
Inheritance Check 4	Password Character Set Complex	Passed
Inheritance Check 5	Password Change Frequency 2 Months	Passed
Inheritance Check 6	Password Change Frequency 6 Months	Passed
Inheritance Check 7	Password Change Frequency 1 Year	Passed
Inheritance Check 8	Email Setting Normal	Passed
Inheritance Check 9	Email Setting Strict	Passed
Inheritance Check 10	Browser Setting Normal	Passed
Inheritance Check 11	Browser Setting Strict	Passed
Inheritance Check 12	Protect With ACL True	Failed
Inheritance Check 13	Allow Writing Passwords True	Failed
Inheritance Check 14	Lock or Logoff Policy True	Failed
Inheritance Check 15	No Email Attachment True	Failed
Inheritance Check 16	Remote Authentication True	Failed
Inheritance Check 17	Accept PKI Certs True	Failed
Inheritance Check 18	Use One Time Password True	Failed
Inheritance Check 19	Use Biometrics True	Failed

Table 1. Inheritance Check Test Results

The value of these tests is mostly seen in actual game play. It is more cost effective to make the default component procedural changes before purchasing any components. This saves time and frustration by eliminating the need to select each of these settings for several components after they have been purchased.

10. Win Trigger Test Scenarios

This series of scenarios was written to verify that the win triggers that were considered for use in the Area 91 scenario actually worked as advertised. Table 2 lists the conditions and triggers tested and the results of the tests:

Tagname	Testing	Results
MaxCashOnHand	Win condition MaxCashOnHand = 10500	Passed
AvgCash	Win condition AvgCash > 10500	Passed
MinCashOnHand	Win condition MinCashOnHand < 20000	Passed
TimeCondition	Win condition TimeCondition = 10 (units is hours)	Passed
TimeCondition	Win condition TimeCondition = 72 (units is hours)	Passed
UserHappiness	Win condition Patrick UserHappiness < 95 (percentage)	Passed
AvgUserHappiness	Win condition AvgUserHappiness < 95 (percentage)	Passed
AvgUserProd	Win condition AvgUserProd > 95 (percentage)	Passed
UserProductivity	Win condition Patrick UserProductivity > 95 (percentage)	Passed
UserFailsGoal	Win condition UserFailsGoal: Patrick fails asset goal	Passed
AssignedComputerHas	Win condition Patrick Work PC has offsitebackup	Passed
MinCashOnHand	Win condition MinCashOnHand > 10100	Failed
MaxCashOnHand and TimeCondition	MaxCashOnHand = 10500 and TimeCondition = 72 (3 days)	Passed
MinCashOnHand and TimeCondition	MinCashOnHand > 10100 and TimeCondition = 72	Failed
TimeCondition and UserHappiness	TimeCondition = 72 and Patrick UserHappiness < 95	Passed
TimeCondition or UserHappiness	TimeCondition = 72 or Patrick UserHappiness < 95	Passed
TimeCondition or UserHappiness	TimeCondition = 72 or Patrick UserHappiness > 95	Passed

Table 2. Win Trigger Test Results

Note that the two failed tests used the MinCashOnHand trigger. In these cases, it makes no sense to test for the minimum cash on hand to be greater than a certain amount. This trigger was designed to test for falling below a certain level. In order to test for going above a certain cash level, the MaxCashOnHand should be used.

11. Summary

This chapter outlined the testing accomplished on the CyberCIEGE game engine. The first section showed the three solutions developed to test expected results against actual results for the Area 91 scenario. The second section detailed the smaller cases written to test specific aspects of the game engine. The following chapter concludes this thesis and outlines future work that remains to be accomplished.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION AND RECOMMENDATIONS

A. RECOMMENDATIONS

1. CyberCIEGE Game Play Issues

Due to the delay of the release of a playable version of the game, a few game play issues were encountered during the course of this thesis. These issues represent areas of recommended improvement to the CyberCIEGE game which can be incorporated prior to its official release.

a. User Training

The first issue is the game's method of presenting user training. It is possible to have virtual users in a scenario with differing training levels. The game represents this training on a sliding integer scale of 1 to 100, with 1 being the lowest amount of training and 100 being the highest. This number is then used to determine a user's ability to correctly configure any components he is assigned and to follow recommended security procedures. One use of this facet could be to introduce users into a scenario with little or no initial training. The player would then have to purchase training for that user to avoid exposing his network to vulnerability. The player has the option of purchasing training in 1, 5, or 10 integer increments.

The current version of the game (21 April 2004) does not allow for the purchase of training upgrades for individual users. Rather, when training is purchased, the game applies it to all of the users in the scenario. If the scenario has ten users, and 1 unit of training costs $100, then the player must spend $1,000 to buy training for all ten users. This becomes expensive quickly for the player, especially if there is only one user who actually needs more training. Due to the prohibitive costs associated with buying training for all of the users in a scenario, this feature of the game cannot be utilized realistically.

b. Background Checks

The second issue involves background checks for the virtual users in the game. The game has two places that provide for the purchase of background checks. They are both located on the Game Tab. The player can select either the Clearances or

Groups button and be presented with an opportunity to buy higher background checks for users. The Clearances dialog window allows for the purchase of background checks based on a user's security clearance. The Groups dialog window is based on the discretionary groups to which a user belongs. The game does not differentiate users who have a clearance based on their DAC group and those who have one based on their Secrecy label. For instance, suppose that User X belongs to DAC Group A which has an initial background check of Low, and a Security Clearance B which has no initial background check. The game still lets the player buy a Low background check under the Clearances dialog window even though User X already has a Low background check.

The confusion arises from allowing these background checks to be purchased on two different screens. This functionality should be consolidated to a single screen where the player has a listing of all users in the scenario along with their corresponding background check levels. The player could then purchase background checks on an individual basis.

c. Asset Usage Changes

The final issue revolves around the use of asset usage change triggers in the scenario definition files. One of the primary factors of the Area 91 scenario was the implementation of changing asset goals for the virtual users. Every user has certain asset goals which represent the assets that the user wants to access. Defined in the SDF is a target usage amount which is the percentage of that user's time that he wishes to utilize to accomplish that goal. For instance, a target usage amount of 60 means that the user wants to spend 60 percent of his time on that asset goal.

The asset usage change trigger changes the target usage amount for a user's asset goal. The target usage can be increased or decreased. The trigger has a parameter that the scenario writer uses to define the new target amount.

A limitation of the game is that asset goals cannot be added to a user dynamically during the course of a game. The user must start the scenario with any asset goals that may be necessary. If the scenario designer wishes to have a user with no initial goals and add them during the course of the game, he must define that user as having the required asset goals and give the user a target usage amount of zero. This should tell the

game that the user wishes to spend zero amount of his time achieving that goal and should not list this as an asset goal failure until such time as the target usage amount rises above zero.

The game does not see the zero target usage amounts as a successful asset goal. As a result, all users with zero target usage amounts are penalized in productivity and the associated availability costs for that asset goal are assessed against the player.

The Area 91 scenario depends heavily on the ability to have zero target usage goals for several users. Because the game engine counts these as failures, the dynamic aspect of the scenario could not be fully tested.

The game should be changed to allow for asset goals to be dynamically added to users as a scenario progresses.

2. Future Work

The size and complexity of a scenario such as this one allows for a multitude of possible learning objectives and improvements to scenario design. Even slight modifications to the scenario definition file can dramatically influence the playability of each scenario. Due to the focus on MAC and DAC, many other beneficial security topics which could have been introduced were omitted.

The most obvious area in need of future work is the testing of the proposed solutions to the scenario, as described in Chapter IV. Once the dynamic aspect of changing asset usage amounts is resolved, the scenario can be fully run and tested.

Another avenue for future work would revolve around the introduction of a multilevel electronic mail system. In this system, users' e-mail would be divided into security classes. The player would then have to implement a system that allowed users of varying clearances to communicate with each other over this system.

In addition, another layer of complexity could be added to this scenario by the introduction of integrity labels. The educational goals could then be expanded to include all three components of network security: integrity, confidentiality, and availability.

Finally, further testing needs to be done on the scenario itself. This would involve giving the game and the scenario to people and measuring if it achieves the desired educational goal of teaching the security concepts associated with MAC, DAC, and Multilevel networking.

B. CONCLUSION

This thesis set out to demonstrate that it is possible to write a scenario for the CyberCIEGE game that teaches the concepts of mandatory and discretionary access control in a multilevel network. A scenario intended to achieve this objective was created. Additional work needs to be done to determine if this is actually true. Subsequent versions of the game engine should make this possible. The game seems to provide the tools necessary to educate the players on these topics.

A secondary goal was to test the CyberCIEGE game engine for expected results using scenario definition files. This thesis experienced many results which improved the game. Through the development of nearly sixty scenario definition files, many aspects of the CyberCIEGE game engine were tested and many flaws and glitches were identified and corrected. Due to the complexity of a large scenario, not all of the testing of the proposed solutions could be accomplished.

As security awareness, training, and education becomes more critical to the safety of DoD networks, the value of simulation-based computer games like CyberCIEGE will continue to expand. This game and its accompanying scenarios may prove to be invaluable in the struggle to keep networks safe, not only from outside attack, but also from the threat of poor user training.

APPENDIX A – SCENARIO SOLUTIONS

A. SINGLE NETWORK SOLUTION

The following are the steps necessary to implement the single network solution for the Area 91 scenario:

a) Entire Office Zone:
    a. Check Enforce Password Policy - $100
    b. Check Guard at Door - $150
    c. Check Patrolling Guard - $150
    d. Check Visual Inspection - $100
    e. Check Key Lock - $24
    f. Check Badges Required - $250
    g. Total spent: $774
b) Nightingale Zone
    a. Check Enforce Password Policy - $100
    b. Check Receptionist Present - $100
    c. Check Guard at Door - $150
    d. Check Patrolling Guard - $150
    e. Check Visual Inspection - $100
    f. Check Key Lock - $24
    g. Check Cypher Lock - $442
    h. Check Prohibit Media - $100
    i. Check Prohibit Phones - $100
    j. Check Poor Zone Alarm - $1400
    k. Check Expensive Iris Scanner - $750
    l. Check Badges Required - $250
    m. Total spent: $3666
c) Fender Zone

    a. Repeat steps from (b)
    b. Total $3666

d) Sensitive Zone
    a. Check Enforce Password Policy - $100
    b. Check Patrolling Guard - $150
    c. Check Key Lock - $24
    d. Total spent: $274

e) No Class Zone
    a. Repeat steps from (d)
    b. Total $274

f) Total spent on zone changes: $8,654

g) Click on Office Tab
    a. Click on ITStaff Button
    b. Hire Mr. Gray, Officer Dan and Officer Bob

The next area to look at is user training. The lowest training setting of a single user is Michael with 69. Click on the button to purchase high user training. This will increase the training level of all users by 10 points, bringing Michael up to 79.

h) Total spent on user training: $27,500

Once these criteria have been met satisfactorily, begin to look at meeting the users' asset goals. The scenario begins with four users with goals that need to be met. They are: 1) Brent – Modify the Daily Report; 2) Michael – Modify the Daily Report, and Read and Write Work E-Mail; 3) Janet – Modify the Daily Report, Read the Daily Report Checklist, Read and Write Work E-Mail, and Read the Administrative Files, and 4) Greg – Modify the Administrative Files and Read and Write Work E-Mail.

The three users with a shared goal of modifying the Daily Report are Brent, Michael, and Janet. The daily report is classified at the Secret Level. The solution puts

the asset Daily Report on a server. Brent, Michael, and Janet will be given workstations and placed on the network along with the server with the Daily Report on it. This meets all of Brent's current goals.

Michael, Janet, and Greg would all like to read and write e-mail. The solution is to place the Work E-Mail asset on the previously purchased server. Greg will now be provided with a workstation. This meets all of Michael's and Greg's current goals.

Finally, since Janet is the only user with the goal of reading the Daily Report Checklist, put the asset directly on her workstation and ensure that she has access to it. This completes Janet's current goals.

i) Purchase a Blato server and place in the Secret zone - $15,000
j) On component tab, assign Daily Report asset to this server and give the Managers group remote access and ACL access to the asset.
k) Purchase 3 Blato workstations and place them into Brent, Michael, and Janet's workspaces - $5,100
l) Place the Work E-Mail asset on the Blato server. Give Area91 group remote access to server.
m) Purchase a Blato workstation and place it into Greg's workspace - $1700. Put the Admin Files asset on this machine and give managers remote access. Add managers onto ACL for asset.
n) On the network tab, ensure that all machines are on the SLAN network. Ensure that Brent has access to the Fender zone.
o) On the Component tab, assign the Daily Report Checklist asset to Janet's workstation and give her access on the asset ACL.
p) Total spent on i-o; $21,800
q) Grand total before unpausing the game: $57,954

The game should now be unpaused and allowed to run for five days. The next thing to happen will be a pop up message stating that it is now day 5 and user goals have changed. The money should also be adjusted to reflect a new research grant.

On the fifth day, the several users will have asset goals that change. They are: 1) Peter – Modify Internet Research, Read and Write Work E-mail; 2) Mary – Modify Internet Research, Read and Write Work E-Mail; 3) Jessica – Modify Research Database, Read and Write Work E-Mail; and 4) Brent – Read Research Database, Read and Write Work E-Mail, Read Biochip Schematics.

Use the server to house the Scientific Research Database, the Biochip Schematics, and the Biochip Test Results.

Since Brent already has a machine, simply ensure that the Scientific Research Database asset has Brent on the ACL. This should satisfy all of Brent's current goals.

Buy workstations for Peter, Mary, and Jessica. Connect these machines to the network. This should satisfy Peter and Mary's shared goal of modifying the Internet Research Database and the rest of their goals as well.

r) On the Component Tab, assign the Scientific Research Database, the Biochip Schematics, and the Biochip Test Results to the server
s) Purchase 3 Blato Desktop Selects and place them into Peter, Mary, and Jessica's workspaces - $5,100
t) On the networks tab, ensure that all machines are on the SLAN network.
u) Total for steps r-t: $5,100

The game should be unpaused again and allowed to run until the tenth day, when more users will have changing asset goals. The money should also be increased by another research grant.

The following is a list of the users with new asset goals: 1) Ivan – Read Biochip Schematics, Modify Biochip Test Results, Modify Research Database, Read Internet Research, and Read and Write Work E-Mail; 2) Michael – Read Biochip Schematics; 3) Jonathan – Modify Biochip Schematics, Read Biochip Test Results, Read Internet Research, and Read and Write Work E-Mail.

Buy a workstation for Ivan and Jonathan. Put them on the network. Give Jonathan and Ivan access to the server. Michael already has a machine with a network connection, so simply ensure the ACLs allow him access to the Biochip Test Results asset.

v) Purchase 2 Blato Desktop Selects and place them into Ivan and Jonathan's workspaces - $3,400
w) On the networks tab, ensure that all machines are on the SLAN network.
x) Total for steps v-w: $3,400

The game should now be unpaused and allowed to run until the fifteenth day. A pop up message will inform of an increase in cash. The users' goals have changed.

The following is a list of users with new asset goals: 1) Hector – Read and Write Work E-Mail, Read Internet Research, Modify Research Database, Modify Biochip Test Results, and Read Mind Control Formula; 2) Patrick – Read Internet Research, Read Research Database, Read Fluoride Database,, Read and Write Work E-Mail, Modify Mind Control Formula; and 3) Brent – Read Mind Control Formula.

Place the Formula and the Fluoride Database on the server.

Buy workstations for Patrick and Ivan. Ensure they are on the network.

Since Brent already has a machine, simply ensure that he has permission to access the Formula.

y) On the component tab, assign the Mind Control Formula and the Fluoride Production Database to the server. Ensure the Scientists group has permission to the asset, as well as Brent.
z) Purchase 2 Blato Desktop Selects and place them into Patrick and Ivan's workspaces - $3,400
aa) On the networks tab, ensure that all machines are on the SLAN network.
bb) Total for steps y-aa - $3,400

Unpause the game and let it finish running for the thirty days.

B. SEPARATE NETWORKS SOLUTION

The proposed solution makes all zone and default component procedural security changes before any components are purchased. After clicking on the Zone tab, areas to look at are access lists to the various zones, physical security settings, and minimum and maximum secrecy labels. Also need to consider hiring of security guards and IT staff. The exact list of changes is as follows:

a) Entire Office Zone:
    a. Check Enforce Password Policy - $100
    b. Check Guard at Door - $150
    c. Check Patrolling Guard - $150
    d. Check Visual Inspection - $100
    e. Check Key Lock - $24
    f. Check Badges Required - $250
    g. Total spent: $774
b) Nightingale Zone
    a. Check Enforce Password Policy - $100
    b. Check Receptionist Present - $100
    c. Check Guard at Door - $150
    d. Check Patrolling Guard - $150
    e. Check Visual Inspection - $100
    f. Check Key Lock - $24
    g. Check Cypher Lock - $442
    h. Check Prohibit Media - $100
    i. Check Prohibit Phones - $100
    j. Check Poor Zone Alarm - $1400
    k. Check Expensive Iris Scanner - $750
    l. Check Badges Required - $250
    m. Total spent: $3666
c) Fender Zone
    a. Repeat steps from (b)

b. Total $3666

d) Sensitive Zone
    a. Check Enforce Password Policy - $100
    b. Check Patrolling Guard - $150
    c. Check Key Lock - $24
    d. Total spent: $274
e) No Class Zone
    a. Repeat steps from (d)
    b. Total $274
f) Total spent on zone changes: $8,654
g) Click on Office Tab
    a. Click on ITStaff Button
    b. Hire Mr. Gray, Officer Dan and Officer Bob

The next area to look at is user training. The lowest training setting of a single user is Michael with 69. Click on the button to purchase high user training. This will increase the training level of all users by 10 points, bringing Michael up to 79.

h) Total spent on user training: $27,500

Once these criteria have been met satisfactorily, begin to look at meeting the users' asset goals. The scenario begins with four users with goals that need to be met. They are: 1) Brent – Modify the Daily Report; 2) Michael – Modify the Daily Report, and Read and Write Work E-Mail; 3) Janet – Modify the Daily Report, Read the Daily Report Checklist, Read and Write Work E-Mail, and Read the Administrative Files, and 4) Greg – Modify the Administrative Files and Read and Write Work E-Mail.

The three users with a shared goal of modifying the Daily Report are Brent, Michael, and Janet. The daily report is classified at the Secret Level. The solution puts the asset Daily Report on a server. Brent, Michael, and Janet will be given workstations

and a connection to a network with components whose only security label is Secret. The Daily Report server will also be placed on this network. This meets all of Brent's current goals.

Michael, Janet, and Greg would all like to read and write e-mail. Since the Work E-Mail asset is classified Sensitive, and Michael and Janet are already on a network with Secret labels, this solution does not allow these users to fully meet this asset goal by giving them a connection to the network with the E-Mail server. Instead, they will have physical access to the zone containing the asset and will have to use a separate terminal.

Greg will be provided with a single level machine. Since all of his asset goals are at the Sensitive level, the Work E-Mail asset will be placed on Greg's workstation allowing him to complete his goal of reading and writing his e-mail. The Administrative Files asset will also be placed on Greg's machine completing all of his goals.

Finally, since Janet is the only user with the goal of reading the Daily Report Checklist, the asset will be put directly on her workstation. This completes Janet's current attainable goals in this solution.

i) Purchase Blato server and place in the Secret zone - $15,000
j) On component tab, assign Daily Report asset to this server and give the Managers group remote access and ACL access to the asset.
k) Purchase 3 Blato Desktop Selects and place them into Brent, Michael, and Janet's workspaces - $5,100
l) Purchase a Blato Desktop Select and place it into Greg's workspace - $1700. Put the Work E-Mail and Admin Files assets on this machine and give managers remote access. Add managers onto ACL for assets.
m) On the network tab, make SLAN connections for Brent, Michael, and Janet's workstations. Put Greg's machine on the ULAN network.
n) On the Component tab, assign the Daily Report Checklist asset to Janet's workstation and give her access on the asset ACL.
o) Total spent on i-n; $21,800
p) Grand total before unpausing the game: $57,954

The game should now be unpaused and allowed to run for five days. The next thing to happen will be a pop up message stating that it is now day 5 and user goals have changed. The money should also be adjusted to reflect a new research grant.

On the fifth day, the several users will have asset goals that change. They are: 1) Peter – Modify Internet Research, Read and Write Work E-mail; 2) Mary – Modify Internet Research, Read and Write Work E-Mail; 3) Jessica – Modify Research Database, Read and Write Work E-Mail; and 4) Brent – Read Research Database, Read and Write Work E-Mail, Read Biochip Schematics.

Use the Daily Report server to house the Scientific Research Database since it is also classified Secret. Buy another server and place the Biochip Schematics and Biochip Test Results on it. Place it in the Nightingale zone.

Since Brent already has a machine on the SLAN, he will automatically be able to access the Scientific Research Database after giving him access to the asset. Brent will only be able to meet his goal of reading the Biochip Schematics by allowing him physical access to the Nightingale zone with the server in it, thus keeping separation of networks while still being able to be partially productive. This should satisfy all of Brent's current goals.

Buy workstations for Peter, Mary, and Jessica. Put Peter and Mary's machines on the ULAN, giving them access to the E-mail server. Place the Internet router on the ULAN as well. This should meet all of Peter and Mary's goals.

Jessica's machine will be placed on the SLAN. This will disallow a network connection to the E-Mail server, but will enable her to reach her goal of modifying the Research Database.

q) On the Component Tab, assign the Scientific Research Database to the server with the Daily Report on it.
r) Purchase a Green Shade Server and place it into the Nightingale Zone - $30,000

s) On the component Tab, assign the Biochip Schematics and the Biochip Test Results to the Green Shade Server.
t) Purchase 3 Blato Desktop Selects and place them into Peter, Mary, and Jessica's workspaces - $5,100
u) On the networks tab, assign Peter and Mary's machines to the ULAN. Assign Jessica's machine to the SLAN. Assign the Internet Router machine to the ULAN.
v) Total for steps r-v: $35,100

The game should be unpaused again and allowed to run until the tenth day, when more users will have changing asset goals. The money should also be increased by another research grant.

The following is a list of the users with new asset goals: 1) Ivan – Read Biochip Schematics, Modify Biochip Test Results, Modify Research Database, Read Internet Research, and Read and Write Work E-Mail; 2) Michael – Read Biochip Schematics; 3) Jonathan – Modify Biochip Schematics, Read Biochip Test Results, Read Internet Research, and Read and Write Work E-Mail.

Buy a workstation for Ivan and Jonathan. Put these workstations on the NLAN. Give Jonathan and Ivan access to the server.

Michael will only be able to reach his new goal by granting him physical access to the Nightingale zone.

w) Purchase 2 Blato Desktop Selects and place them into Ivan and Jonathan's workspaces - $3,400
x) On the networks tab, assign Ivan and Jonathan's machines to the NLAN.
y) Total for steps z-aa: $3,400

The game should now be unpaused and allowed to run until the fifteenth day. A pop up message will inform of an increase in cash. The users' goals have changed.

The following is a list of users with new asset goals: 1) Hector – Read and Write Work E-Mail, Read Internet Research, Modify Research Database, Modify Biochip Test Results, and Read Mind Control Formula; 2) Patrick – Read Internet Research, Read Research Database, Read Fluoride Database, Read and Write Work E-Mail, Modify Mind Control Formula; and 3) Brent – Read Mind Control Formula.

Buy a server and place the Formula and the Fluoride Database on it. Place the server in the Fender zone.

Buy workstations for Patrick and Ivan. Put them on the FLAN.

Since Brent already has a machine on the SLAN, grant him access to the Fender zone to partially fulfill his asset goal of reading the Formula.

z) Purchase a Green Shade Server and place it into the Fender Zone - $30,000.
aa) On the component tab, assign the Mind Control Formula and the Fluoride Production Database to the Fender server.
bb) Purchase 2 Blato Desktop Selects and place them into Patrick and Ivan's workspaces - $3,400
cc) On the networks tab, assign the Fender server, Patrick's workstation, and Hector's workstation to the FLAN.
dd) Total for steps z-cc - $33,400

Unpause the game and let it finish running for the thirty days.

C. MULTILEVEL NETWORK SOLUTION

The exact list of steps for the multilevel network solution is as follows:

a) Entire Office Zone:
    a. Check Enforce Password Policy - $100
    b. Check Guard at Door - $150
    c. Check Patrolling Guard - $150
    d. Check Visual Inspection - $100

    e. Check Key Lock - $24
    f. Check Badges Required - $250
    g. Total spent: $774

b) Nightingale Zone
    a. Check Enforce Password Policy - $100
    b. Check Receptionist Present - $100
    c. Check Guard at Door - $150
    d. Check Patrolling Guard - $150
    e. Check Visual Inspection - $100
    f. Check Key Lock - $24
    g. Check Cypher Lock - $442
    h. Check Prohibit Media - $100
    i. Check Prohibit Phones - $100
    j. Check Poor Zone Alarm - $1400
    k. Check Expensive Iris Scanner - $750
    l. Check Badges Required - $250
    m. Total spent: $3666

c) Fender Zone
    a. Repeat steps from (b)
    b. Total $3666

d) Sensitive Zone
    a. Check Enforce Password Policy - $100
    b. Check Patrolling Guard - $150
    c. Check Key Lock - $24
    d. Total spent: $274

e) No Class Zone
    a. Repeat steps from (d)
    b. Total $274

f) Total spent on zone changes: $8,654

g) Click on Office Tab

a. Click on ITStaff Button
b. Hire Mr. Gray, Officer Dan and Officer Bob

The next area to look at is user training. The lowest training setting of a single user is Michael with 69. Click on the button to purchase high user training. This will increase the training level of all users by 10 points, bringing Michael up to 79.

h) Total spent on user training: $27,500

Once these criteria have been met satisfactorily, begin to look at meeting the users' asset goals. The scenario begins with four users with goals that need to be met. They are: 1) Brent – Modify the Daily Report; 2) Michael – Modify the Daily Report, and Read and Write Work E-Mail; 3) Janet – Modify the Daily Report, Read the Daily Report Checklist, Read and Write Work E-Mail, and Read the Administrative Files, and 4) Greg – Modify the Administrative Files and Read and Write Work E-Mail.

The three users with a shared goal of modifying the Daily Report are Brent, Michael, and Janet. The daily report is classified at the Secret Level. The solution puts the asset Daily Report on a server. Brent, Michael, and Janet will be given multilevel machines and a connection with Secret labels will be established to the server with the Daily Report on it. This meets all of Brent's current goals.

Michael, Janet, and Greg would all like to read and write e-mail. The solution is to purchase a server and place the Work E-Mail asset on it. Greg will now be provided with a single level machine since all of his asset goals are at the same security label – sensitive. All three users will be given a connection to the server with the e-mail asset on it. This meets all of Michael's and Greg's current goals.

Finally, since Janet is the only user with the goal of reading the Daily Report Checklist, put the asset directly on her workstation and ensure that she has access to it. This completes Janet's current goals.

i) Purchase Blato server and place in the Secret zone - $15,000

j) On component tab, assign Daily Report asset to this server and give the Managers group remote access and ACL access to the asset.
k) Purchase 3 Secure Shade Desktops and place them into Brent, Michael, and Janet's workspaces - $9,000
l) Purchase Mail Appliace Server and assign Work E-Mail asset to it and place in the Sensitive Zone - $5,000. Give Area91 group remote access to server.
m) Purchase a Blato Desktop Select and place it into Greg's workspace - $1700. Put the Admin Files asset on this machine and give managers remote access. Add managers onto ACL for asset.
n) On the network tab, make SensLAN connections from these four users' machines to the e-mail server, and make SECLAN connections for Brent, Michael, Janet, and the Daily Report Server. Ensure that Brent has access to the Fender zone.
o) On the Component tab, assign the Daily Report Checklist asset to Janet's workstation and give her access on the asset ACL.
p) Total spent on i-o; $30,700
q) Grand total before unpausing the game: $66,854

The game should now be unpaused and allowed to run for five days. The next thing to happen will be a pop up message stating that it is now day 5 and user goals have changed. The money should also be adjusted to reflect a new research grant.

On the fifth day, the several users will have asset goals that change. They are: 1) Peter – Modify Internet Research, Read and Write Work E-mail; 2) Mary – Modify Internet Research, Read and Write Work E-Mail; 3) Jessica – Modify Research Database, Read and Write Work E-Mail; and 4) Brent – Read Research Database, Read and Write Work E-Mail, Read Biochip Schematics.

Use the Daily Report server to house the Scientific Research Database since it is also classified Secret. Buy another server and place the Biochip Schematics and Biochip Test Results on it. Place it in the Nightingale zone.

Since Brent already has a machine, simply establish a Secret LAN connection to the server with the Scientific Research Database on it and give him remote access. Establish a Nightingale connection to the server with the Biochip Schematics and give him remote access. And establish a Sensitive LAN connection to the E-Mail server and give him remote access if necessary. (The Area91 group should already have DAC access) This should satisfy all of Brent's current goals.

Buy multilevel machines for Peter, Mary, and Jessica. Establish a Sensitive LAN connection from each of their machines to the E-Mail server. Establish Unclassified LAN connections from Peter and Mary's machines to the router that is connected to the Internet Research Database. This should satisfy Peter and Mary's shared goal of modifying the Internet Research Database and the rest of their goals as well.

Establish a Secret LAN connection from Jessica's machine to the server with the Scientific Research Database on it. This should satisfy all of Jessica's goals.

r) On the Component Tab, assign the Scientific Research Database to the server with the Daily Report on it.
s) Purchase a Green Shade Server and place it into the Nightingale Zone - $30,000
t) On the component Tab, assign the Biochip Schematics and the Biochip Test Results to the Green Shade Server.
u) Purchase 3 Secure Shade Desktop Machines and place them into Peter, Mary, and Jessica's workspaces - $9,000
v) On the networks tab, assign Brent's machine to the NLAN, SECLAN, SENSLAN, and ULAN networks. Assign Peter's machine to the ULAN and SENSLAN networks. Assign Mary's machine to the ULAN and SENSLAN networks as well. Assign Jessica's machine to the SECLAN and SENSLAN networks.
w) Total for steps r-v: $39,000

The game should be unpaused again and allowed to run until the tenth day, when more users will have changing asset goals. The money should also be increased by another research grant.

The following is a list of the users with new asset goals: 1) Ivan – Read Biochip Schematics, Modify Biochip Test Results, Modify Research Database, Read Internet Research, and Read and Write Work E-Mail; 2) Michael – Read Biochip Schematics; 3) Jonathan – Modify Biochip Schematics, Read Biochip Test Results, Read Internet Research, and Read and Write Work E-Mail.

Buy a multilevel machine for Ivan and Jonathan. Establish Nightingale LAN connections to the server with the Schematics and Test Results assets on it. Give Jonathan and Ivan access to the server. Finally, establish a Sensitive LAN connection from these two users' machines to the E-Mail server.

Michael already has a machine, so simply establish a Nightingale connection to the network with the machine housing the Biochip Test Results asset.

x) Purchase 2 Secure Shade Desktops and place them into Ivan and Jonathan's workspaces - $6000
y) On the networks tab, assign Ivan's machine to the NLAN, SECLAN, SENSLAN and ULAN networks. Assign Michael's machine to the NLAN. Assign Jonathan's machine to the NLAN, SENSLAN, and ULAN networks.
z) Total for steps z-aa: $6000

The game should now be unpaused and allowed to tun until the fifteenth day. A pop up message will inform of an increase in cash. The users' goals have changed.

The following is a list of users with new asset goals: 1) Hector – Read and Write Work E-Mail, Read Internet Research, Modify Research Database, Modify Biochip Test Results, and Read Mind Control Formula; 2) Patrick – Read Internet Research, Read Research Database, Read Fluoride Database,, Read and Write Work E-Mail, Modify Mind Control Formula; and 3) Brent – Read Mind Control Formula.

Buy a server and place the Formula and the Fluoride Database on it. Place the server in the Fender zone.

Buy multilevel machines for Patrick and Ivan. Establish Fender LAN connections to the server with the Formula and Fluoride Database. Establish Secret LAN connections to the server with the Research Database. Establish Sensitive LAN connections to the E-Mail server. And finally, establish Unclassified LAN connections to the Internet router. This should satisfy all of the goals for Patrick and Ivan.

Since Brent already has a machine, simply establish a Fender connection to the server with the Formula on it.

aa) Purchase a Green Shade Server and place it into the Fender Zone - $30,000.

bb) On the component tab, assign the Mind Control Formula and the Fluoride Production Database to the Fender server.

cc) Purchase 2 Secure Shade Desktops and place them into Patrick and Ivan's workspaces - $6,000

dd) On the networks tab, assign the Fender server to the FLAN. Assign Patrick's machine to the FLAN, SECLAN, SENSLAN, and ULAN. Assign Hector's machine to the FLAN, SECLAN, SENSLAN, and ULAN. Assign Brent's machine to the FLAN.

ee) Total for steps aa-dd - $36,000

Unpause the game and let it finish running for the thirty days.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B – AREA 91 FULL SCENARIO

```
// Area 91 Full Scenario

Organization:
        Name: Area_91_Secret_Projects_Facility          :end
        Title: Area 91 Simple Scenario 1    :end
        StartMoney: 70000   :end
        Budget: 25000       :end
        StartMonth: 10              :end
        StartDay: 1         :end
        StartHour: 7        :end
        StartMinute: 00             :end
        WorkspaceFile: area91workspace.txt
        ProfitSharing: 10   :end
        QuitText: Thanks for playing.:end
:end

OPTIONS:
UseScenarioCatalogItems: Yes        :end
:end

//Define the entire site

Site:
        Name: Simple Office         :end
        Description: Planet Desmid's premiere secret projects research facility
:end
:end

Camera:
        ViewCenterX:            45      :end
        ViewCenterY:            41      :end
        ViewAmountBack:  70     :end
        ViewAmountUp:           37      :end
:end

        //*****************************************************************
******

//      Zones

// This zone defines the whole work center
```

Zone:

Name: Entire Office :end

Description: This is the main work floor which most of the users have access to. :end

Site: Simple Office :end

//Begin procedural security

HoldsUserAsset: true :end

MaxSecrecyLabel: Secret :end

MinSecrecyLabel: Unclassified :end

AccessList: *.Area91 :end AccessMode: YYXX :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: true:end

ApplyPatches: true :end

LeaveMachinesOn: false :end

NoPhysicalModifications: true :end

UserBackup: false :end

//End procedural security

Receptionist: false :end

GuardatDoor: false :end

PatrollingGuard: false:end

ProhibitMedia: false :end

ProhibitPhoneDevices: false :end

ExpensivePerimeterAlarms: false :end

Re-enforcedWalls: true :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
        Secrecy: Secret        :end
        PermittedUsers: *.Area91     :end
        Network: SLAN        :end
        ULC:  20  57 :end
        LRC:  68  25  :end
:end

// This zone defines the Nightingale work area

Zone:
        Name: Nightingale Zone       :end
        Description: This is the work zone for the Nightingale Projects.     :end
        Site: Simple Office          :end
        Art: UpLeftZone.tga          :end

        //Begin procedural security
        HoldsUserAsset: true  :end
        MaxSecrecyLabel: Nightingale        :end
        MinSecrecyLabel: Nightingale        :end
        AccessList: *.Scientists  :end  AccessMode: YYXX  :end
        ProtectWithACL: true:end
        WriteDownPasswords: false  :end
        LockorLogoff:  true   :end
        PasswordLength: long:end
        PasswordCharacterSet: complex       :end
        PasswordChangeFrequency: two        :end
        NoEmailAttachmentExecute: true      :end
        NoExternalSoftware: true  :end
        NoUseofModems: true         :end
        NoWebMail: true       :end
        NoMediaLeaveZone: true      :end
        UpdateAntiVirus: true:end
        ApplyPatches: true     :end
        LeaveMachinesOn: false       :end
        NoPhysicalModifications: true         :end
        UserBackup: false      :end
        //End procedural security
        Receptionist: false      :end
        GuardatDoor: false     :end
        PatrollingGuard: false:end
        ProhibitMedia: false   :end
        ProhibitPhoneDevices: false  :end
        ExpensivePerimeterAlarms: false      :end
        Re-enforcedWalls: true         :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
        Secrecy: Nightingale   :end
        PermittedUsers: *.Scientists   :end
        Network: NLAN         :end
        ULC:   20   50 :end
        LRC:  41  45   :end
:end

// This zone defines the Fender work area

Zone:
        Name: Fender Zone    :end
        Description: This is the work zone for the Fender Projects.  :end
        Site: Simple Office              :end
        Art: LowRightZone.tga                  :end

        //Begin procedural security
        HoldsUserAsset: true  :end
        MaxSecrecyLabel: Fender :end
        MinSecrecyLabel: Fender :end
        AccessList: *.Scientists  :end  AccessMode: YYXX  :end
        ProtectWithACL: true:end
        WriteDownPasswords: false  :end
        LockorLogoff:  true    :end
        PasswordLength: long:end
        PasswordCharacterSet: complex        :end
        PasswordChangeFrequency: two        :end
        NoEmailAttachmentExecute: true      :end
        NoExternalSoftware: true  :end
        NoUseofModems: true          :end
        NoWebMail: true       :end
        NoMediaLeaveZone: true       :end
        UpdateAntiVirus: true:end
        ApplyPatches: true     :end
        LeaveMachinesOn: false       :end
        NoPhysicalModifications: true          :end
        UserBackup: false      :end
```

```
        //End procedural security

        Receptionist: false      :end
        GuardatDoor: false     :end
        PatrollingGuard: false:end
        ProhibitMedia: false   :end
        ProhibitPhoneDevices: false  :end
        ExpensivePerimeterAlarms: false      :end
        Re-enforcedWalls: true         :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
        Secrecy: Nightingale  :end
        PermittedUsers: *.Scientists  :end
        Network: FLAN        :end
        ULC:  49  39 :end
        LRC:  68  26  :end
:end

// This zone defines the Sensitive work area

Zone:
        Name: Sensitive Zone:end
        Description: This is the work zone for Sensitive research and users.:end
        Site: Simple Office              :end
        Art: LowLeftZone.tga          :end

        //Begin procedural security
        HoldsUserAsset: true  :end
        MaxSecrecyLabel: Sensitive :end
        MinSecrecyLabel: Unclassified :end
        AccessList: *.Area91  :end  AccessMode: YYXX  :end
        ProtectWithACL: true:end
        WriteDownPasswords: false  :end
        LockorLogoff:  true    :end
        PasswordLength: short         :end
        PasswordCharacterSet: moderate      :end
        PasswordChangeFrequency: six        :end
```

NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseofModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: true:end
ApplyPatches: true :end
LeaveMachinesOn: false :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security

Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false:end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
Re-enforcedWalls: true :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
Secrecy: Sensitive :end
PermittedUsers: *.Area91 :end
Network: Internet :end
ULC: 20 39 :end
LRC: 33 26 :end
:end

// This zone defines the Unclassified work area

Zone:
Name: No Class Zone :end
Description: This is the work zone for Intenet research and users who have no clearance. :end

Site: Simple Office :end
Art: UpRightZone.tga :end
//Begin procedural security

```
        HoldsUserAsset: true  :end
        MaxSecrecyLabel: Unclassified :end
        MinSecrecyLabel: Unclassified :end
        AccessList: *.Area91  :end  AccessMode: YYXX  :end
        ProtectWithACL: true:end
        WriteDownPasswords: false  :end
        LockorLogoff:  true   :end
        PasswordLength: short         :end
        PasswordCharacterSet: any   :end
        PasswordChangeFrequency: twelve  :end
        NoEmailAttachmentExecute: true    :end
        NoExternalSoftware: true  :end
        NoUseofModems: true         :end
        NoWebMail: true      :end
        NoMediaLeaveZone: true     :end
        UpdateAntiVirus: true:end
        ApplyPatches: true    :end
        LeaveMachinesOn: false      :end
        NoPhysicalModifications: true        :end
        UserBackup: false     :end
        //End procedural security

        Receptionist: false     :end
        GuardatDoor: false    :end
        PatrollingGuard: false:end
        ProhibitMedia: false  :end
        ProhibitPhoneDevices: false  :end
        ExpensivePerimeterAlarms: false     :end
        Re-enforcedWalls: true        :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
        Secrecy: Unclassified :end
        PermittedUsers: *.Area91     :end
        Network: Internet      :end
        ULC:  55  57 :end
        LRC:  68  44  :end
:end
```

// This zone defines the offsite location that will be used for an Internet connection.

Zone:
Name: Internet Zone :end
Description: This is the Internet Service Provider for the Research Facility :end
Site: Simple Office :end
Art: offsitezone.tga :end
//Begin procedural security
HoldsUserAsset: true :end
Static: true :end
ProtectWithACL: false :end
WriteDownPasswords: false :end
LockorLogoff: false :end
PasswordLength: short :end
PasswordCharacterSet: moderate :end
PasswordChangeFrequency: never :end
NoEmailAttachmentExecute: false :end
NoExternalSoftware: false :end
NoUseofModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: false :end
UpdateAntiVirus: false :end
ApplyPatches: false :end
LeaveMachinesOn: false :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security

Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: true :end
KeyLockonDoor: true :end
CipherLockonDoor: true :end
ExpensiveIrisScanner: true :end

```
            ModerateIrisScanner: true      :end
            Badges: true    :end
            Secrecy: Unclassified :end
            Network: Internet       :end
            ULC:   93   25 :end
            LRC:  104  14   :end
        :end

        //*****************************************************************
**************************
        //     Networks


        // Fender Local Area Network = FLAN

        Network:
            Name: FLAN  :end
            NetID: 6.6.6.0 :end
        :end

        //Nightingale Local Area Network = NLAN
        Network:
            Name: NLAN :end
            NetID: 7.7.7.0 :end
        :end

        //Sensitive/Secret Local Area Network = SLAN

        Network:
            Name: SENSLAN               :end
            NetID: 10.10.10.0       :end
        :end

        //Unclassified Local Area Network = ULAN
        Network:
            Name: ULAN          :end
            NetID: 9.9.9.0          :end
        :end

        //Network for offsite connection to Internet

        Network:
            Name: OffsiteNet       :end
            NetID: 200.200.200.0 :end
            Static: True            :end
```

```
:end

//*************************************************************************
**************************
//    Secrecy Labels
//Define the Fender Secrecy Tag

Secrecy:
        Name: Fender :end
        Level: 64       :end
        Category: 1     :end
        SecrecyValue: 1000000       :end
        AttackerValue: 500    :end
        InitialBackGroundCheck: High        :end
:end

Secrecy:
        Name: Nightingale     :end
        Level: 64       :end
        Category: 2     :end
        SecrecyValue: 500000        :end
        AttackerValue:          300     :end
        InitialBackGroundCheck: High        :end
:end

Secrecy:
        Name: Secret  :end
        Level: 52       :end
        SecrecyValue: 10000  :end
        AttackerValue: 150    :end
        InitialBackGroundCheck: Medium    :end
:end

Secrecy:
        Name: Sensitive       :end
        Level: 36       :end
        SecrecyValue: 5000   :end
        AttackerValue: 50     :end
        InitialBackGroundCheck: Low         :end
:end

Secrecy:
        Name: Unclassified    :end
        Level: 10       :end
        SecrecyValue: 1000   :end
```

```
        AttackerValue: 15      :end
        InitialBackGroundCheck: None        :end
    :end

    //*****************************************************************
**************************************
    //    DAC GRoups

    //Initial DAC groups

    DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:     None   :end

        Group: Managers       :end
        InitialBackGroundCheck: None        :end

        Group: Area91                 :end
        InitialBackgroundCheck:     None   :end
    :end

    //*****************************************************************
**************************************
    //    Assets
    //Asset is the mind control formula

    Asset:
        Name: Liquid Fluoride Mind Control Formula        :end
        Description: The scientists at Area 91 have a formula for producing a
liquid fluoride-based mind control serum.  They have code named any research related to
this formula as Fender. All Fender assets are the most valuable possessed by this
organization.  When placed into the water supply, it reduces the ability to make decisions,
making the surrounding population more docile and easier to control.  This formula
consists of the mathematical models and detailed chemical properties of the formula. If
this formula falls into enemy hands, the results would be catastrophic. Enemy scientists
could formulate ways of detecting the presence of the liquid, or could formulate
antidotes.  Also, the formula could be quickly used as a weapon against us, causing our
demise. Only users cleared to Fender should have access to this data. :end

        IsInstantiated: false    :end
        HasDac: true             :end
        Secrecy: Fender                :end
        DOSMotive: 300                 :end
        AvailabilityPenalty:   100000          :end
        CostList:
```

Access: *.Public :end
AccessMode: YNNN :end
Cost: 100000 :end
AttackerMotive: 501 :end
:end
:end //asset

Asset:
Name: Liquid Fluoride Production Database :end
Description: This asset contains an inventory of every batch of mind control serum produced at Area 91. It also lists each corresponding production serial number, storage location, and/or release site for each batch of serum. While the military leaders consider this project to be their greatest accomplishment, the scientists have run into a snag. After years of testing, they have concluded that the formula doesn't actually work. Since this database reflects the failure of this formula, the scientists would prefer not to allow project management access. There will be $10,000 in costs related to disruption should an access violation occur; and management has a fairly high motive to read this database. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Fender :end
DOSMotive: 300 :end
AvailabilityPenalty: 100000 :end
CostList:
Access: *.Public :end
AccessMode: YNNN :end
Cost: 100000 :end
AttackerMotive: 200 :end
:end //costlist

CostList:
Access: *.Managers :end
AccessMode: YYNN :end
Cost: 10000 :end
AttackerMotive: 200 :end
:end //Costlist
:end //asset

Asset:
Name: Human Biochip Implant Schematics :end
Description: The designs for a computer chip that can be placed into humans for tracking purposes are the next most valuable asset held by the military on this planet. These chips are usually implanted into unsuspecting civilians during routine vaccinations at local doctor's offices. The military uses a super-computer to catalog and

track the movements of the entire population. If the schematics were to become known, our enemies would possess the ability to mask or spoof the signals coming from the biochips. Also, they could track the population themselves, as well as produce their own implants. This research has been code named Nightingale and only users with this clearance should have access to this data. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Nightingale :end
DOSMotive: 250 :end
AvailabilityPenalty: 30000 :end
CostList:
Access: *.Public :end
AccessMode: YYNN :end
Cost: 10000 :end
AttackerMotive: 300 :end
:end //costlist
:end //asset

Asset:
Name: Human Biochip Implant Test Data :end
Description: This asset consists of the latest test results for the working version of the biochip designs. It is based on a modeling program that uses the Biochip Schematics. Since this database reflects how far behind the Nightingale project is, the scientists would prefer to keep it from the Planetary Council which means keeping it out of the daily report. If this information is leaked to the Council's informants, it will cost the enterprise $5,000 in disruption and the informants have a motive to access this information should the opportunity present itself. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Nightingale :end
DOSMotive: 250 :end
AvailabilityPenalty: 30000 :end
CostList:
Access: *.Public :end
AccessMode: YYNN :end
Cost: 10000 :end
AttackerMotive: 200 :end
:end //costlist

Costlist:
Access: *.Managers :end
AccessMode: YYNN :end
Cost: 5000 :end

AttackerMotive: 100 :end
:end
:end //asset

Asset:
Name: Daily Report :end
Description: This report is prepared for Planet Desmid's Ruling Planetary Council to keep it aware of the daily ongoing operations at Area 91. The facility's funding for its projects depends completely on favorable progress reports to the Council. Since these reports blame program slip-ups on the scientists and glosses over management's role in any blunders, morale among the scientists would be totally jeopardized if these reports are disclosed to them. This would cause $3,000 worth of damage to Area 91's funds and the scientists have a higher than average motive to read these reports. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Secret :end
DOSMotive: 200 :end
AvailabilityPenalty: 20000 :end
CostList:
Access: *.Public :end
AccessMode: YNNN :end
Cost: 100000 :end
AttackerMotive: 200 :end
:end //costlist

CostList:
Access: *.Scientists :end
AccessMode: YNNN :end
Cost: 3000 :end
AttackerMotive: 200 :end
:end
:end //asset

Asset:
Name: Daily Report Checklist :end
Description: This checklist contains the necessary steps to create the daily report. The Ruling Council is extremely particular about the content and format of the daily report. This checklist must be followed exactly or the daily report will be rejected by the council and funding for the facility will be suspended. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Sensitive :end

DOSMotive: 150 :end
AvailabilityPenalty: 10000 :end
CostList:
Access: *.Public :end
AccessMode: YYNN :end
Cost: 10000 :end
AttackerMotive: 200 :end
:end //costlist
:end //asset

Asset:
Name: Scientific Research Database :end
Description: Some of the scientists are not cleared to the code name projects but nonetheless are able to conduct research indirectly related to the projects. This database represents the ongoing research conducted by these scientists with only a Secret clearance. The Fender and Nightingale users assign research topics related to their work and will need access to the database to track the ongoing progress of these topics. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Secret :end
DOSMotive: 200 :end
AvailabilityPenalty: 60000 :end
CostList:
Access: *.Public :end
AccessMode: YYNN :end
Cost: 100000 :end
AttackerMotive: 200 :end
:end //costlist

//Jonathan wants to read this asset
CostList:
Access: Jonathan :end
AccessMode: YNNN :end
Cost: 50000 :end
AttackerMotive: 300 :end
:end //costlist
:end //asset

Asset:
Name: Administrative Files :end
Description: Check the user tab to learn which of the managers is responsible for the day to day operations at the facility. This asset represents the personnel records, interoffice memorandums, service contracts, and other administrative

data required to keep the facility operational. Without this repository of files, the facility would cease operations resulting in a total shut-down. :end

---

IsInstantiated: false :end
HasDac: false :end
Secrecy: Sensitive :end
DOSMotive: 50 :end
AvailabilityPenalty: 5000 :end
:end //asset

Asset:
Name: Internet Research :end
Description: Posing one of your greatest security risks is your connection to the Internet. New users assigned to your facility are given the responsibility of conducting open source research, pending verification of their security clearance. You begin with a router in one of your zones with an Internet connection to an offsite machine containing this asset. The challenge will be to keep data from flowing out of your facility. Improper security configurations could allow outsiders access to confidential data on your network. Be careful what machines you allow to be connected to this asset. :end

IsInstantiated: true :end
HasDac: false :end
Secrecy: Unclassified :end
DOSMotive: 100 :end
AvailabilityPenalty: 1000 :end

:end //asset

Asset:
Name: Work E-Mail :end
Description: All of your users would like to be able to read and write e-mail. Communication between the members of the various project teams is vital for productivity and the morale of the users. Providing all users access to this asset will have the greatest impact on the happiness of your people. :end
IsInstantiated: false :end
HasDac: true :end
Secrecy: Sensitive :end
DOSMotive: 100 :end
AvailabilityPenalty: 10000 :end
CostList:
Access: *.Public :end
AccessMode: YYNN :end
Cost: 1000 :end

AttackerMotive: 10 :end
:end //costlist

:end //asset

//**********
****

// Asset Goals
//Define asset goals

AssetGoal:
Name: Modify Mind Control Formula :end
Description: This goal requires modification of the Liquid Fluoride Mind Control Formula. As the scientists continue to experiment with the formula, they will need to change the mathematical models and chemical properties stored in the formula. This goal will require the use of a word processor application. :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end
:end //asset list

AvailabilityCostPenalty: 1000000 :end

:end //asset goal

AssetGoal:
Name: Read Mind Control Formula :end
Description: This goal requires read access to the Liquid Fluoride Mind Control Formula. Some of the scientists who are responsible for working on the liquid fluoride production database will need read access to this asset in order to properly track changes made in the formula and update the database accordingly. This goal will require the use of a word processor application. :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YXXX :end
:end //asset list
AvailabilityCostPenalty: 500000 :end

:end //asset goal

AssetGoal:
Name: Read and Write Work E-Mail :end
Description: This goal requires read and write access to the Work E-Mail asset. Note that this asset is labeled as sensitive and that all of the users have this goal. The scientists and managers at the facility are dependent upon e-mail access to

communicate between each other. If users fail this goal, their happiness will be greatly diminished. This goal will require the use of an e-mail client. :end

Asset:
Name: Work E-Mail :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 20000 :end

:end //asset goal

AssetGoal:
Name: Modify Fluoride Database :end
Description: This goal requires modification of the Liquid Fluoride Mind Control Database. The scientists who use this database will also require read access to Liquid Fluoride Mind Control Formula. :end
Asset:
Name: Liquid Fluoride Production Database :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 500000 :end

:end //asset goal

AssetGoal:
Name: Read Fluoride Database :end
Description: This goal requires read access to the Liquid Fluoride Mind Control Database. The scientists responsible for modification of the formula would like to keep track of the changes made to this database. :end
Asset:
Name: Liquid Fluoride Production Database :end
AccessMode: YXXX :end
:end //asset list
AvailabilityCostPenalty: 400000 :end
:end //asset goal

AssetGoal:
Name: Read Research Database :end
Description: This goal requires read access to the Scientific Research Database. Each of the code word scientists has various research projects they have handed down to the scientists only cleared for secret work. These lower cleared researchers modify the Scientific Research Database and the code word scientists require read access to track the progress of their projects. :end
Asset:
Name: Scientific Research Database :end
AccessMode: YXXX :end

:end //asset list
AvailabilityCostPenalty: 250000 :end
:end //asset goal

AssetGoal:
Name: Read Internet Research :end
Description: This goal requires read access to the Internet Research asset. The scientists who possess a clearance would like to keep track of the current progress of the Research being conducted at the unclassified level :end
Asset:
Name: Internet Research :end
AccessMode: YXXX :end
:end //asset list
AvailabilityCostPenalty: 100000 :end

:end //asset goal

AssetGoal:
Name: Modify Internet Research :end
Description: This goal requires modification of the Internet Research asset. Failure to meet this goal will result in an almost total loss of productivity of the unclassified users. This is a collaborative effort that will fail unless all users who have this goal are able to modify this asset. :end
Shared: True :end
Asset:
Name: Internet Research :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 30000 :end
:end //asset goal

AssetGoal:
Name: Modify Biochip Schematics :end
Description: This goal requires modification of the Human Biochip Implant Schematics assets. As work progresses on the biochips, the scientists responsible for this project will need to update the schematics to reflect the current working version of the biochip. :end
Asset:
Name: Human Biochip Implant Schematics :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 121 :end
:end //asset goal

AssetGoal:

Name: Read Biochip Schematics :end

Description: This goal requires read access to the Human Biochip Implant Schematics asset. The scientists who track testing results on the biochips will need to be able to read the current schematics so that they may make correct entries into the test results database. Users with this goal will require a word processor application. :end

Asset:

Name: Human Biochip Implant Schematics :end

AccessMode: YXXX :end

:end //asset list

AvailabilityCostPenalty: 121 :end

:end //asset goal

AssetGoal:

Name: Modify Biochip Test Results :end

Description: This goal requires modification of the Human Biochip Implant Test Data. This test data is used in the ongoing experimentation with the biochips. Each new chip design is tested for human compatibility or rejection, transmitter strength, battery life, and adverse health risks in the human subjects. Several humans have been abducted from the planet Earth to accomplish these tests. Users will need a spreadsheet program to accomplish this goal. :end

Asset:

Name: Human Biochip Implant Test Data :end

AccessMode: YXXX :end

:end //asset list

AvailabilityCostPenalty: 121 :end

:end //asset goal

AssetGoal:

Name: Read Biochip Test Results :end

Description: This goal requires read access to the Human Biochip Implant Test Data. The current working version of the biochips is completely dependent upon the interpretation of previous test experiments on the abducted humans. This goal will also require a spreadsheet application in order to succeed. :end

Asset:

Name: Human Biochip Implant Test Data :end

AccessMode: YXXX :end

:end //asset list

AvailabilityCostPenalty: 121 :end

:end //asset goal

AssetGoal:

Name: Modify Daily Report :end

Description: Brent, Janet, and Michael have a shared goal to modify the daily report with a word processor :end

Shared: True :end

Asset:
Name: Daily Report :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 121 :end
:end //asset goal

AssetGoal:
Name: Read Daily Report Checklist :end
Description: Read the daily report checklist with a spreadsheet program :end
Asset:
Name: Daily Report Checklist :end
AccessMode: YXXX :end
:end //asset list
AvailabilityCostPenalty: 121 :end
:end //asset goal

AssetGoal:
Name: Modify Research Database :end
Description: Modify the scientific research database :end
Asset:
Name: Scientific Research Database :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 121 :end
:end //asset goal

AssetGoal:
Name: Read Admin Files :end
Description: Read the Administrative Files :end
Asset:
Name: Administrative Files :end
AccessMode: YXXX :end
:end //asset list
AvailabilityCostPenalty: 121 :end
:end //asset goal

AssetGoal:
Name: Modify Admin Files :end
Description: Modify the Administrative Files :end
Asset:
Name: Administrative Files :end
AccessMode: YXXX :end
:end //asset list

```
            AvailabilityCostPenalty: 121 :end

        :end //asset goal

        //*****************************************************************
*****************************************
        //    Users
        //Define user Patrick, cleared to Fender, member of scientists group

        User:
            Name: Patrick :end
            SecrecyClearance: Fender     :end
            DACGroups:
                Public  :end
                SCIENTISTS  :end
                Area91:end
            :end //DAC groups

            DefaultDAC: SCIENTISTS   :end

            AssetGoal:
                AssetGoalName: Modify Mind Control Formula :end
                TargetUsage:  0       :end
                Happiness:    15      :end
                Productivity:  40     :end
            :end //asset goal

            AssetGoal:
                AssetGoalName: Read and Write Work E-Mail       :end
                TargetUsage:  0       :end
                Happiness:    40      :end
                Productivity:  15     :end
            :end

            AssetGoal:
                AssetGoalName: Read Fluoride Database :end
                TargetUsage:  0       :end
                Happiness:    20      :end
                Productivity:  20     :end
            :end //asset goal

            AssetGoal:
                AssetGoalName: Read Research Database :end
                TargetUsage:  0       :end
                Happiness:    15      :end
```

Productivity: 15 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read Internet Research :end
TargetUsage: 0 :end
Happiness: 10 :end
Productivity: 10 :end
:end //asset goal

Trustworthiness: 88 :end
InitialTraining: 85 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 2 :end
Cost: 1000 :end
Gender: Male :end

UserDescription: Patrick is the inventor of the Liquid Fluoride Mind Control formula and the chief scientist on the Fender project. As the project chief, he is responsible for modification of the formula as research progresses and advancements are made. He also needs to keep tabs on the Fluoride Production Database to ensure correct entries are being made by his assistant, Hector. Patrick also hands out assignments to Jessica, and needs to track her work by having read access to the Scientific Research Database. Patrick would prefer to also have access to the Internet Research if possible. Finally, in order to communicate with Hector and Jessica, as well as the facility management, he needs access to e-mail. :end

:end //user Patrick

User:
Name: Jonathan :end
SecrecyClearance: Nightingale :end

DACGroups:
Public :end
SCIENTISTS :end
Area91:end
:end //DAC groups

DefaultDAC: SCIENTISTS :end

AssetGoal:
AssetGoalName: Modify Biochip Schematics :end

TargetUsage: 0 :end
Happiness: 25 :end
Productivity: 45 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read Biochip Test Results :end
TargetUsage: 0 :end
Happiness: 15 :end
Productivity: 30 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read Internet Research :end
TargetUsage: 0 :end
Happiness: 10 :end
Productivity: 10 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 0 :end
Happiness: 40 :end
Productivity: 15 :end
:end

Trustworthiness: 72 :end
InitialTraining: 86 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 8 :end
Cost: 1000 :end
Gender: Male :end

UserDescription: Jonathan is the lead scientist on the Nightingale project. The Desmid Intelligence Agency delivered the Biochip plans to Jonathan for safekeeping and further research. He may be a bit unscrupulous at times, prone to take shortcuts, and sloppy in his work. He only maintains his position as project leader due to his connections with the Agency. Jonathan's goals are to gather as much information from the various projects in the facility as possible. This includes the Scientific Research Database, even though Patrick is responsible for giving Jessica her work, Jonathan is motivated to try to "sneak a peak" at the work being done. Jonathan needs to read the

latest Biochip Test Results and the Internet Research. In order to communicate with his team, give him access to read and write e-mail. :end

:end //user Jonathan

User:
Name: Brent :end
SecrecyClearance: Fender :end

DACGroups:
Public :end
Managers :end
Area91:end
:end //DAC groups

DefaultDAC: Managers :end

AssetGoal:
AssetGoalName: Read Mind Control Formula :end
TargetUsage: 0 :end
Happiness: 15 :end
Productivity: 20 :end
:end //asset goal

AssetGoal:
AssetGoalName: Modify Daily Report :end
TargetUsage: 40 :end
Happiness: 25 :end
Productivity: 40 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read Research Database :end
TargetUsage: 0 :end
Happiness: 10 :end
Productivity: 15 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read Internet Research :end
TargetUsage: 0 :end
Happiness: 10 :end
Productivity: 10 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 0 :end
Happiness: 40 :end
Productivity: 15 :end
:end

Trustworthiness: 87 :end
InitialTraining: 79 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 3 :end
Cost: 1000 :end
Gender: Male :end

UserDescription: Brent is one of two managers responsible for reporting on the code named projects to the Planetary Council. Brent's area of expertise is the mind control formula. His position as a senior manager dictates that he must have access to the formula and any research being conducted at the Secret level or below. Brent needs to be able to modify the Daily Report simultaneously with Michael and Janet. He also requires the ability to compose e-mail. :end

:end //user Brent

User:
Name: Jessica :end
SecrecyClearance: Secret :end

DACGroups:
Public :end
SCIENTISTS :end
Area91:end
:end //DAC groups

DefaultDAC: SCIENTISTS :end

AssetGoal:
AssetGoalName: Modify Research Database :end
TargetUsage: 0 :end
Happiness: 35 :end
Productivity: 75 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 0 :end
Happiness: 40 :end
Productivity: 25 :end
:end

Trustworthiness: 96 :end
InitialTraining: 72 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 0 :end
Cost: 1000 :end
Gender: Female :end

UserDescription: Jessica is a younger scientist who works for Patrick. He gives her research projects and she tracks her progress on these in the Scientific Research Database. She keeps Patrick informed of her progress by sending coded messages via e-mail. :end

:end //user Jessica

User:
Name: Michael :end
SecrecyClearance: Nightingale :end

DACGroups:
Public :end
Managers :end
Area91:end
:end //DAC groups

DefaultDAC: Managers :end

AssetGoal:
AssetGoalName: Read Biochip Schematics :end
TargetUsage: 0 :end
Happiness: 20 :end
Productivity: 45 :end
:end //asset goal

AssetGoal:
AssetGoalName: Modify Daily Report :end
TargetUsage: 40 :end

Happiness: 20 :end
Productivity: 45 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 15 :end
Happiness: 40 :end
Productivity: 10 :end
:end

Trustworthiness: 92 :end
InitialTraining: 69 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 9 :end
Cost: 1000 :end
Gender: Male :end

UserDescription: Michael is the other senior manager, along with Brent, who is responsible for reporting on the code named projects to the Planetary Council. Michael has been given a Nightingale clearance for the purposes of reporting on the status of the biochip research. As such, he requires read access to the current version of the Biochip Schematics. He needs to modify the Daily Report simultaneously with Brent and Janet. Since Brent handles reporting on the Secret and below projects, the only other goal for Michael is to read and write his e-mail. :end

:end //user Michael

User:
Name: Mary :end
SecrecyClearance: Sensitive :end

DACGroups:
Public :end
SCIENTISTS :end
Area91:end
:end //DAC groups

DefaultDAC: SCIENTISTS :end

AssetGoal:
AssetGoalName: Modify Internet Research :end
TargetUsage: 0 :end

Happiness: 40 :end
Productivity: 80 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 0 :end
Happiness: 60 :end
Productivity: 20 :end
:end //asset goal

Trustworthiness: 96 :end
InitialTraining: 72 :end
Happiness: 75 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 15 :end
Cost: 1000 :end
Gender: Female :end
UserDescription: Mary's main responsibility is to conduct open source research on the Internet. She is handed various topics by Patrick and Jonathan and uses these as a basis for her work. Due to the large number of topics in her current workload, she has been assigned an assistant to split the load. As a result, she and Peter must collaborate together to modify the Internet Research database. She is given her topics through the e-mail system. :end

:end //user Mary

User:
Name: Janet :end
SecrecyClearance: Secret :end

DACGroups:
Public :end
Managers :end
Area91:end
:end //DAC groups

DefaultDAC: Managers :end

AssetGoal:
AssetGoalName: Modify Daily Report :end
TargetUsage: 20 :end
Happiness: 25 :end

Productivity: 20 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read Daily Report Checklist :end
TargetUsage: 10 :end
Happiness: 15 :end
Productivity: 10 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 15 :end
Happiness: 20 :end
Productivity: 15 :end
:end

AssetGoal:
AssetGoalName: Read Admin Files :end
TargetUsage: 30 :end
Happiness: 20 :end
Productivity: 30 :end
:end

Trustworthiness: 96 :end
InitialTraining: 72 :end
Happiness: 75 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 1 :end
Cost: 1000 :end
Gender: Female :end

UserDescription: Janet is the senior editor of the Daily Report. The Planetary Council is extremely conscientious of the formatting and appearance of the report and have given Janet a Checklist to ensure that the report matches their specifications. While Janet shares the responsibility of modifying the report with Brent and Michael, she ultimately ensures that the report makes its way up the chain of command. She also keeps tabs on the Administrative Files to ensure that Greg is fulfilling his requirements as the facility administrative supervisor :end

:end //user Janet

User:
Name: Greg :end
SecrecyClearance: Sensitive :end

DACGroups:
Public :end
Managers :end
Area91:end
:end //DAC groups

DefaultDAC: Managers :end

AssetGoal:
AssetGoalName: Modify Admin Files :end
TargetUsage: 60 :end
Happiness: 25 :end
Productivity: 60 :end
:end //asset goal

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 20 :end
Happiness: 55 :end
Productivity: 20 :end
:end

Trustworthiness: 96 :end
InitialTraining: 72 :end
Happiness: 75 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 16 :end
Cost: 1000 :end
Gender: male :end

UserDescription: Greg is the facility's administrative supervisor. He keeps the facility operating from day to day. He handles all contracts with service providers and all human resource issues such as personnel and finance. He stores all information related to these activities in the Administrative Files asset. He also is responsible for dispensing any bulk e-mails to the facility's users. :end

:end //user Greg

User:
Name: Peter :end

SecrecyClearance: Unclassified :end

DACGroups:
Public :end
Scientists :end
Area91:end
:end //DAC groups

DefaultDAC: Scientists :end

Assetgoal:
AssetGoalName: Modify Internet Research :end
TargetUsage: 0 :end
Happiness: 40 :end
Productivity: 60 :end
:end

Assetgoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 0 :end
Happiness: 60 :end
Productivity: 40 :end
:end

Trustworthiness: 96 :end
InitialTraining: 72 :end
Happiness: 75 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 17 :end
Cost: 1000 :end
Gender: male :end

UserDescription: Peter works closely with Mary to conduct research on the Internet. He has been brought in solely as a means to ease Mary's workload and possesses no security clearance. He has basically been given a desk in a corner and told to stay there while in the facility. He is curious about what goes on the facility and may get caught wandering around from time to time. :end

:end //user Peter

User:
Name: Hector :end
SecrecyClearance: Fender :end

```
DACGroups:
        Public  :end
        Scientists      :end
        Area91:end
:end //DAC groups

DefaultDAC: Scientists      :end

Assetgoal:
        AssetGoalName: Read Mind Control Formula        :end
        TargetUsage:  0       :end
        Happiness:    20      :end
        Productivity: 20      :end
:end

AssetGoal:
        AssetGoalName: Modify Fluoride Database         :end
        TargetUsage:  0       :end
        Happiness:    20      :end
        Productivity: 20      :end
:end

AssetGoal:
        AssetGoalName: Modify Research Database         :end
        TargetUsage:  0       :end
        Happiness:    20      :end
        Productivity: 20      :end
:end

AssetGoal:
        AssetGoalName: Read Internet Research           :end
        TargetUsage:  0       :end
        Happiness:    20      :end
        Productivity: 20      :end
:end

AssetGoal:
        AssetGoalName: Read and Write Work E-Mail       :end
        TargetUsage:  0       :end
        Happiness:    20      :end
        Productivity: 20      :end
:end

Trustworthiness: 96   :end
InitialTraining: 72   :end
```

Happiness: 75 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 4 :end
Cost: 1000 :end
Gender: male :end

UserDescription: Hector is Patrick's lab assistant and is in charge of updating the Fluoride Production Database as new batches of the serum are produced. Hector catalogues each batch of serum and tags them for tracking purposes. Patrick allows Hector to follow his work on the formula, so he will require read access to that asset. Hector also monitors the Scientific Research Database for any breakthroughs and would also like to access the Internet Research asset. Hector also requires the ability to read and write e-mail. :end

:end //user Hector

User:
Name: Ivan :end
SecrecyClearance: Nightingale :end

DACGroups:
Public :end
Scientists :end
Area91:end
:end //DAC groups

DefaultDAC: Scientists :end

AssetGoal:
AssetGoalName: Read Biochip SChematics :end
TargetUsage: 0 :end
Happiness: 20 :end
Productivity: 20 :end
:end

AssetGoal:
AssetGoalName: Modify Biochip Test Results :end
TargetUsage: 0 :end
Happiness: 20 :end
Productivity: 20 :end
:end

AssetGoal:
AssetGoalName: Modify Research Database :end

TargetUsage: 0 :end
Happiness: 20 :end
Productivity: 20 :end
:end

AssetGoal:
AssetGoalName: Read Internet Research :end
TargetUsage: 0 :end
Happiness: 20 :end
Productivity: 20 :end
:end

AssetGoal:
AssetGoalName: Read and Write Work E-Mail :end
TargetUsage: 0 :end
Happiness: 20 :end
Productivity: 20 :end
:end

Trustworthiness: 96 :end
InitialTraining: 72 :end
Happiness: 75 :end
Productivity: 100 :end
Skill: 95 :end
PosIndex: 10 :end
Cost: 1000 :end
Gender: male :end

UserDescription: Ivan coordinates all testing and research on the current working version of the biochips. He reads the current schematic, performs his tests and then takes the test results and inputs them into a spreadsheet for correlation and comparison analysis with previous versions of the chip design. Ivan also conducts some research at the Secret level and stores these in the Scientific Research Database. He also requires access to the Internet Research and the ability to compose e-mail. :end

:end //user Hector

//**********
****

// IT Staff and Security

// Officer Bob: Security Guard

User:

```
        Name: Officer Bob           :end
        Dept: Security          :end
        DACGroups:
                Public  :end
        :end

        Trustworthiness:    95      :end
        InitialTraining:    70      :end
        DaysTillAvailable:  0       :end
        Happiness:      90          :end
        Productivity:   75          :end
        Skill:          80          :end
        PosIndex:       12          :end
        Cost:   600                 :end
        Gender:         Male                :end
        UserDescription: Bob likes to patrol  :end
:end

//Officer Dan: Security Guard

User:
        Name: Officer Dan           :end
        Dept: Security          :end
        DACGroups:
                Public  :end
        :end
        Trustworthiness:    97      :end
        InitialTraining:    88      :end
        DaysTillAvailable:  0       :end
        Happiness:      92          :end
        Productivity:   87          :end
        Skill:          93          :end
        PosIndex:       12          :end
        Cost:   1200                :end
        Gender:         Male                :end
        UserDescription: Dan likes donuts.  :end
:end

//Mr. Gray: IT Staff

User:
        Name: Mr. Gray              :end
        Dept: Tech              :end
        DACGroups:
                Public  :end
```

```
            :end
            Trustworthiness:    100    :end
            InitialTraining:    98     :end
            DaysTillAvailable:  0      :end
            Happiness:    99           :end
            Productivity: 99           :end
            Skill:        99           :end
            HISupportSkill: 98         :end
            HWSupportSkill: 97         :end
            SWSupportSkill: 92         :end
            PosIndex:     5            :end
            Cost:  2100                :end
            Gender:       Male                 :end
            UserDescription: Mr. Gray will take care of all IT issues for the facility.
        :end
        :end

        //*****************************************************************
*****************************************
        //    Components

        //Define Server at offsite location with Internet Asset instantiated on it

        Component:
            Name: Internet Access Machine      :end
            IsTemplate: false          :end

            Description: This machine represents access to the Internet. A router from
the No Class zone connects to this machine to allow access to the Internet Research asset.
        :end
            AssetProtection:      true    :end
            HW: Blato Desktop Select   :end
            Static: true               :end
            Availability:  100         :end
            Resale: 200                :end
            OS: Populos V9 Desktop             :end
            BlockRemovableMedia: true  :end
            UpdatePatches: AUTOMATIC           :end
            UpdateAntiVirus: AUTOMATIC         :end
            PosIndex: 11               :end
            Network:
                Name: OffsiteNet       :end
            :end
            Assets: Internet Research      :end
            AccessListRemote: *.Area91 :end
```

```
            ComponentProceduralSettings:
                  PasswordLength: short         :end
                  PasswordCharacterSet: Moderate      :end
                  PasswordChangeFrequency: never    :end
                  NoPhysicalModifications: true         :end
            :end
      :end

      //Define Router in unclass zone with connection to the offsite server

      Component:
            Name: Internet Gateway                :end
            IsTemplate: false               :end
            Description: This router is the connection to the Internet and the only way
to reach the Internet Research Asset. :end
            HW: Bit Flipper                       :end
            Static: false                 :end
            Availability: 100             :end
            Resale: 10                    :end
            PosIndex: 17                  :end
            Network:
                  Name: Internet                  :end
            :end
            Network:
                  Name: OffsiteNet      :end
            :end
      :end



      //Define Items to be used as the component catalog

      Component:
            Name:  Blato Desktop Select :end
            IsTemplate:    true :end
            Description: Packed with applications, memory and disk :end
            AssetProtection:        true :end
            HW:  Blato Desktop Select :end
            Cost: 1700 :end
            Resale: 200 :end
            Maintenance: 100 :end
            Availability: 99 :end
            OS:  Populos V9 Desktop      :end
      :end
```

Component:
Name: Targo Worksaver :end
IsTemplate: true :end
Description: Full suite of productivity software, adequate memory and disk. :end
AssetProtection: true :end
HW: Targo Worksaver :end
Cost: 1700 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
:end

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

Component:
Name: Secure Shade Desktop:end
IsTemplate: true :end
Description: Similar to the Blato Desktop, but includes the Secure Shade OS. :end
AssetProtection: true :end
HW: Blato Desktop Select :end
Cost: 5000 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Green Shade Core :end
:end

Component:
Name: Lunitos AFOS :end

IsTemplate: true :end
Description: Sleek colorful desktop machine with adequate memory and disk :end
AssetProtection: true :end
HW: Lunitos AFOS :end
Cost: 2300 :end
Resale: 300 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Lunitos Desktop :end
:end

Component:
Name: Targo Server :end
IsTemplate: true :end
Description: Full featured server with the worlds most popular operating system. :end
AssetProtection: true :end
HW: Targo Server :end
Cost: 15000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
:end

Component:
Name: Blato Server :end
IsTemplate: true :end
Description: Full featured server with the worlds most popular operating system. :end
AssetProtection: true :end
HW: Blato Server :end
Cost: 15000 :end
Resale: 5000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
:end

Component:
Name: Green Shade Server :end
IsTemplate: true :end
Description: Server class machine with the Secure Shade Server high assurance operating system :end

AssetProtection: true :end
HW: Green Shade Server :end
Cost: 30000 :end
Resale: 20000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Server :end
:end

Component:
Name: Mail Appliance :end
IsTemplate: true :end
Description: Basic Email server. :end
AssetProtection: true :end
HW: Targo Server :end
Software: Do Mail :end
Cost: 5000 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
:end

Component:
Name: Populos Letter Pusher :end
IsTemplate: true :end
Description: More popular Email Server with the most well-known operating system. :end
AssetProtection: true :end
HW: Blato Server :end
Software: Populus Letter Pusher :end
Cost: 20000 :end
Resale: 8000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
:end

Component:
Name: Web Appliance :end
IsTemplate: true :end
Description: Simple web server :end
AssetProtection: true :end
HW: Twist Off Server :end
Software: Populos Web Slave :end

Cost: 1500 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Jar Lid Server :end
:end

Component:
Name: Populos Internet Slave :end
IsTemplate: true :end
Description: Web Server with the most popular operating system. :end
AssetProtection: true :end
HW: Blato Server :end
Software: Populos Web Slave :end
Cost: 10000 :end
Resale: 2000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end
:end

Component:
Name: Bit Flipper Router :end
IsTemplate: true :end
Description: High performance router :end
HW: Bit Flipper :end
Cost: 200 :end
Resale: 75 :end
Maintenance: 25 :end
Availability: 99 :end
OS: FlipOS :end
:end

Component:
Name: Bit Flipper Switch :end
IsTemplate: true :end
Description: Best Selling Switch :end
HW: Bit Flipper Switch :end
Cost: 500 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: FlipOS :end
:end

Component:
	Name: Swenthabit :end
	IsTemplate: true :end
	Description: Ordinary LAN switch :end
	HW: Swenthabit :end
	Cost: 500 :end
	Resale: 200 :end
	Maintenance: 100 :end
	Availability: 99 :end
	OS: FlipOS :end
:end

Component:
	Name: Five Inches of Asbestos :end
	IsTemplate: true :end
	Description: Best selling firewall :end
	HW: Five Inches of Asbestos :end
	Cost: 900 :end
	Resale: 200 :end
	Maintenance: 100 :end
	Availability: 99 :end
	OS: Populos V9 Desktop :end
:end

Component:
	Name: Bit Flipper Border :end
	IsTemplate: true :end
	Description: Full featured firewall :end
	HW: Bit Flipper Border :end
	Cost: 200 :end
	Resale: 100 :end
	Maintenance: 100 :end
	Availability: 99 :end
	OS: Populos V9 Desktop :end
:end

Component:
	Name: Wire Stuff :end
	IsTemplate: true :end
	Description: High quality hub with high reliability :end
	HW: Wire Stuff :end
	Cost: 150 :end
	Resale: 100 :end
	Maintenance: 100 :end
	Availability: 99 :end

:end

Component:
Name: Box with Wires :end
IsTemplate: true :end
Description: General purpose hub :end
HW: Box with Wires :end
Cost: 90 :end
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
:end

//**********
// Briefings

Briefing: Welcome to Area 91. This is Planet Desmid's premiere secret projects research facility. Please see the game tab for a full briefing. (PARAGRAPH)

Area 91 houses two major research projects. The first is code named Fender. The Fender project revolves around the production of a liquid-fluoride based mind control serum. When introduced into the water supply, the surrounding population becomes highly susceptible to outside influences. The scientists at the facility have a formula for creating the serum, along with a database that tracks the various production batches of the serum. These assets are worth $1,000,000 to the organization and attackers have a very high motive for compromising everything Fender related. You can find more information about these Fender-related projects on the asset tab.

The second project is code named Nightingale. This project is concerned with the manufacture of tracking devices that can be implanted into humans. These devices are small biological microchips easily introduced into the human blood stream through an injection. The project team has the schematics for these biochips and a database of test results related to the experiments with the biochips. These assets are worth $500,000 to the organization and attackers are extremely motivated to disclose anything with this secrecy label. Look for more information on the asset tab.

Also look for details of other assets and the associated goals that the users in your facility have on the asset tab.

Area 91 has only recently been built and has no existing computer networks. Your mission as the Computer Networks Officer is to supervise the procurement and installation of the necessary components to allow the facility's users to do their work. There are two user groups co-located in your facility: scientists and managers. The scientists' goals revolve around accessing the various projects in the facility, while the managers' goals are to keep the facility running and to ensure that the projects stay on track. You can find more details about each user on the user tab.

You have been given initial funding by the Ruling Planetary Council of $1,000,000. You will also receive a monthly budget for your IT department of $2,000. If you use your funds wisely, the Council may give you more research grants later.

In order to win this scenario: you have to keep the facility going for thirty days without losing all of your money. If your balance falls below zero, you will lose. (PARAGRAPH)

Strategies and Tips:

On the user tab, each user has his asset goals listed along with their associated target usage amounts. You will notice as you progress through the scenario that some users have target usages of zero. This number will change as time goes by, so keep an eye on them.

Initially, only a few of your users have asset goals that need to be met immediately. Concentrate your efforts on meeting the needs of those users who are involved with creating the daily situational report. This daily report keeps the Planetary Council apprised of the progress of the projects at Area 91.

After 5 days, users with goals to access Internet Research and Scientific Research Databases will change. Also, note that the needs of the users responsible for the daily report may change as well, so be sure to check everyone's goals on the fifth day.

After 10 days, the asset goals of the Nightingale project team will change. They will need to be provided with the necessary resources to access their assets. Look for details on the user and asset tabs.

On day 15, your Fender project team will have goals that will need to be met.

Also, for further help, you may press 'e' to bring up the game encyclopedia.

```
:end

        DebriefWin:  You win.  :end

        DebriefLose: You Lose.  :end

    //*****************************************************************
*****************************************
    //    Conditions

    Conditions:

    //*************                    Time                    Conditions
*****************************************************************


        // Will go off on the fifth day. To be used to change user target asset goals
        Condition:
            ConditionClass: TimeCondition    :end
            Tagname:    FifthDay    :end
            Parameter:  120         :end
        :end

        Condition:
            ConditionClass: TimeCondition    :end
            Tagname:    TenthDay    :end
            Parameter:  240         :end
        :end

        Condition:
            ConditionClass: TimeCondition    :end
            Tagname:    FifteenthDay :end
            Parameter:  360         :end
        :end

        //This thirty day condition is used for the win trigger.
        Condition:
            ConditionClass: TimeCondition    :end
            Tagname:    ThirtiethDay :end
            Parameter:  720         :end
        :end

    //**************    Productivity    and    Asset    Goal    Conditions
*********************************************************
```

```
        //If any user falls below 50 productivity
        Condition:
                ConditionClass: UserProductivity    :end
                ConditionText: *                    :end
                Tagname: UsersUnproductive                  :end
                Parameter: 0                        :end
                Parameter: 50                       :end
        :end

    //**********                    Cash                    Conditions
**********************************************************************

        //This is the money falls below zero condition, used with the lose trigger
        Condition:
                ConditionClass: MinCashOnHand           :end
                Tagname:    MoneyBelowZero              :end
                Parameter:  0                       :end
                Parameter:  1                       :end
        :end

    :end //of Conditions Section

    //**********************************************************************
****************************************
    //  Triggers

    Triggers:

    //***************                   Win                     Triggers
**********************************************************************

        //Win if thirty days goes by.
        Trigger:
                TriggerClass:  WinTrigger   :end
                TriggerName: ThirtyDaysGoneBy   :end
                FrequencyInDays:    1       :end
                TriggerText: Congratulations! You have lasted for thirty days.
Press "L" to see your results log.      :end
                ConditionList: ThirtiethDay  :end
        :end

    //***************                   Lose                    Triggers
**********************************************************************

        //Lose if money falls below zero
```

```
Trigger:
        TriggerClass:  LoseTrigger    :end
        TriggerName: MoneyAllGone         :end
        FrequencyInDays:      1         :end
        TriggerText: You have lost all of your money. :end
        ConditionList: MoneyBelowZero      :end
:end

    //***************          Change          Asset          Usage          Triggers
**************************************************

        //THis section changes the asset usages for users with Internet or Scientific
Research asset goals

Trigger:
        TriggerClass: ChangeAssetUsageTrigger      :end
        TriggerName: PeterInternetChange   :end
        FrequencyInDays:      1                :end
        TriggerText:    Peter                  :end
        SecondTriggerText: Modify Internet Research        :end
        Parameter:      60                     :end
        ConditionList: FifthDay                        :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger      :end
        TriggerName: PeterEMailChange      :end
        FrequencyInDays:      1                :end
        TriggerText:    Peter                  :end
        SecondTriggerText: Read and Write Work E-Mail   :end
        Parameter:      40                     :end
        ConditionList: FifthDay                        :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger      :end
        TriggerName: MaryInternetChange   :end
        FrequencyInDays:      1                :end
        TriggerText:    Mary                   :end
        SecondTriggerText: Modify Internet Research        :end
        Parameter:      80                     :end
        ConditionList: FifthDay                        :end
:end

Trigger:
```

TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: MaryEMailChange :end
FrequencyInDays: 1 :end
TriggerText: Mary :end
SecondTriggerText: Read and Write Work E-Mail :end
Parameter: 20 :end
ConditionList: FifthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: JessicaDatabaseChange :end
FrequencyInDays: 1 :end
TriggerText: Jessica :end
SecondTriggerText: Modify Research Database :end
Parameter: 75 :end
ConditionList: FifthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: JessicaEMailChange :end
FrequencyInDays: 1 :end
TriggerText: Jessica :end
SecondTriggerText: Read and Write Work E-Mail :end
Parameter: 25 :end
ConditionList: FifthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: BrentDatabaseChange :end
FrequencyInDays: 1 :end
TriggerText: Brent :end
SecondTriggerText: Read Research Database :end
Parameter: 15 :end
ConditionList: FifthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: BrentInternetChange :end
FrequencyInDays: 1 :end
TriggerText: Brent :end
SecondTriggerText: Read Internet Research :end

```
        Parameter:      10                      :end
        ConditionList: FifthDay                 :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: BrentEMailChange           :end
        FrequencyInDays:    1                   :end
        TriggerText:    Brent                   :end
        SecondTriggerText: Read and Write Work E-Mail   :end
        Parameter:      15                      :end
        ConditionList: FifthDay                 :end
:end

//This section changes the day 10 Biochip / Nightingale users' goals

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: IvanBiochipChange          :end
        FrequencyInDays:    1                   :end
        TriggerText:    Ivan                    :end
        SecondTriggerText: Read Biochip Schematics      :end
        Parameter:      20                      :end
        ConditionList: TenthDay                 :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: IvanTestResultsChange              :end
        FrequencyInDays:    1                   :end
        TriggerText:    Ivan                    :end
        SecondTriggerText: Modify Biochip Test Results  :end
        Parameter:      20                      :end
        ConditionList: TenthDay                 :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: IvanDatabaseChange         :end
        FrequencyInDays:    1                   :end
        TriggerText:    Ivan                    :end
        SecondTriggerText: Modify Research Database     :end
        Parameter:      20                      :end
        ConditionList: TenthDay                 :end
:end
```

```
Trigger:
        TriggerClass: ChangeAssetUsageTrigger     :end
        TriggerName: IvanInternetChange           :end
        FrequencyInDays:    1                     :end
        TriggerText:   Ivan                       :end
        SecondTriggerText: Read Internet Research :end
        Parameter:     20                         :end
        ConditionList: TenthDay                   :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger     :end
        TriggerName: IvanEMailChange              :end
        FrequencyInDays:    1                     :end
        TriggerText:   Ivan                       :end
        SecondTriggerText: Read and Write Work E-Mail   :end
        Parameter:     20                         :end
        ConditionList: TenthDay                   :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger     :end
        TriggerName: MichaelSchematicsChange            :end
        FrequencyInDays:    1                     :end
        TriggerText:   Michael                    :end
        SecondTriggerText: Read Biochip Schematics      :end
        Parameter:     45                         :end
        ConditionList: TenthDay                   :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger     :end
        TriggerName: JonathanSchematicsChange           :end
        FrequencyInDays:    1                     :end
        TriggerText:   Jonathan                   :end
        SecondTriggerText: Modify Biochip Schematics    :end
        Parameter:     45                         :end
        ConditionList: TenthDay                   :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger     :end
        TriggerName: JonathanTestResultsChange          :end
        FrequencyInDays:    1                     :end
```

```
        TriggerText:   Jonathan                    :end
        SecondTriggerText: Read Biochip Test Results    :end
        Parameter:     30                  :end
        ConditionList: TenthDay                    :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger    :end
        TriggerName: JonathanInternetChange            :end
        FrequencyInDays:     1             :end
        TriggerText:   Jonathan                    :end
        SecondTriggerText: Read Internet Research :end
        Parameter:     10                  :end
        ConditionList: TenthDay                    :end
:end


Trigger:
        TriggerClass: ChangeAssetUsageTrigger    :end
        TriggerName: JonathanEMailChange               :end
        FrequencyInDays:     1             :end
        TriggerText:   Jonathan                    :end
        SecondTriggerText: Read and Write Work E-Mail   :end
        Parameter:     15                  :end
        ConditionList: TenthDay                    :end
:end

//This section changes the day 15 Mind Control / Fender users' goals

Trigger:
        TriggerClass: ChangeAssetUsageTrigger    :end
        TriggerName: HectorEMailChange         :end
        FrequencyInDays:     1             :end
        TriggerText:   Hector                  :end
        SecondTriggerText: Read and Write Work E-Mail   :end
        Parameter:     20                  :end
        ConditionList: FifteenthDay                :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger    :end
        TriggerName: HectorInternetChange      :end
        FrequencyInDays:     1             :end
        TriggerText:   Hector                  :end
        SecondTriggerText: Read Internet Research :end
```

```
        Parameter:      20                      :end
        ConditionList: FifteenthDay             :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: HectorDatabaseChange       :end
        FrequencyInDays:    1                   :end
        TriggerText:    Hector                  :end
        SecondTriggerText: Modify Research Database     :end
        Parameter:      20                      :end
        ConditionList: FifteenthDay             :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: HectorProductionDBChange   :end
        FrequencyInDays:    1                   :end
        TriggerText:    Hector                  :end
        SecondTriggerText: Modify Fluoride Database     :end
        Parameter:      20                      :end
        ConditionList: FifteenthDay             :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: HectorFormulaChange        :end
        FrequencyInDays:    1                   :end
        TriggerText:    Hector                  :end
        SecondTriggerText: Read Mind Control Formula    :end
        Parameter:      20                      :end
        ConditionList: FifteenthDay             :end
:end

Trigger:
        TriggerClass: ChangeAssetUsageTrigger   :end
        TriggerName: BrentFormulaChange         :end
        FrequencyInDays:    1                   :end
        TriggerText:    Brent                   :end
        SecondTriggerText: Read Mind Control Formula    :end
        Parameter:      20                      :end
        ConditionList: FifteenthDay             :end
:end

Trigger:
```

TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: PatrickFormulaChange :end
FrequencyInDays: 1 :end
TriggerText: Patrick :end
SecondTriggerText: Modify Mind Control Formula :end
Parameter: 40 :end
ConditionList: FifteenthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: PatrickEMailChange :end
FrequencyInDays: 1 :end
TriggerText: Patrick :end
SecondTriggerText: Read and Write Work E-Mail :end
Parameter: 15 :end
ConditionList: FifteenthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: PatrickProductionDBChange :end
FrequencyInDays: 1 :end
TriggerText: Patrick :end
SecondTriggerText: Read Fluoride Database :end
Parameter: 20 :end
ConditionList: FifteenthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: PatrickDatabaseChange :end
FrequencyInDays: 1 :end
TriggerText: Patrick :end
SecondTriggerText: Read Research Database :end
Parameter: 15 :end
ConditionList: FifteenthDay :end
:end

Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: PatrickInternetChange :end
FrequencyInDays: 1 :end
TriggerText: Patrick :end
SecondTriggerText: Read Internet Research :end

```
                Parameter:      10                      :end
                ConditionList: FifteenthDay                     :end
        :end

    //***************                   Message                 Triggers
**************************************************************

        //Trigger for user productivity below 50
        Trigger:
                TriggerClass: MessageTrigger        :end
                TriggerName: LowProductivityMessage     :end
                FrequencyInDays: 1          :end
                TriggerText: Your users are not being productive! Please ensure
that you are properly meeting their goals.      :end
                ConditionList: UsersUnproductive    :end
        :end

        //Trigger for message about changing user goals on day 5
        Trigger:
                TriggerClass: MessageTrigger        :end
                TriggerName: FiveDayMessage     :end
                FrequencyInDays: 1          :end
                TriggerText: It is now day 5. Check your user goals.:end
                ConditionList: FifthDay     :end
        :end

        //Trigger for message about changing user goals on day 10
        Trigger:
                TriggerClass: MessageTrigger        :end
                TriggerName: TenDayMessage      :end
                FrequencyInDays: 1          :end
                TriggerText: It is now day 10. Check your user goals.       :end
                ConditionList: TenthDay     :end
        :end

        //Trigger for message about changing user goals on day 15
        Trigger:
                TriggerClass: MessageTrigger        :end
                TriggerName: FifteenDayMessage  :end
                FrequencyInDays: 1          :end
                TriggerText: It is now day 15. Check your user goals.       :end
                ConditionList: FifteenthDay :end
        :end
```

```
//******************** Cash Triggers
**********************************************************************

        //The 5, 10, and 15 day conditions will trigger an increase in cash

        Trigger:
                triggerClass: CashTrigger      :end

                TriggerName: FiveDayCashBoost     :end

                FrequencyInDays: 0.5          :end

                TriggerText: You have been given a research grant from the
PLanetary Council of $20,000.          :end

                Parameter: 20000       :end

                ConditionList: FifthDay :end
        :end

        Trigger:
                triggerClass: CashTrigger      :end

                TriggerName: TenDayCashBoost     :end

                FrequencyInDays: 0.5          :end

                TriggerText: You have been given a research grant from the
PLanetary Council of $20,000 for the Nightingale Project.   :end

                Parameter: 20000       :end

                ConditionList: TenthDay :end
        :end

        Trigger:
                triggerClass: CashTrigger      :end

                TriggerName: FiveDayCashBoost     :end

                FrequencyInDays: 0.5          :end

                TriggerText: You have been given a research grant from the
PLanetary Council of $20,000 for the Fender project.          :end
```

```
                    Parameter: 20000        :end

                    ConditionList: FifteenthDay :end
                :end


        :end //of Trigger section

        //*************************************************************************
*****************************************
        //     End of File

        :EndofFile
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C – SMALL SCENARIOS

A. SHARED GOAL SCENARIO

// Area 91 small fully playable scenario. This scenario will have two users with a shared //goal.

// The player will need to provide the proper components to allow the users to reach their //goal.

Organization:

Name: Desmid_Planetary_Forces :end
Title: Area 91 Simple Scenario 1 :end
StartMoney: 30000 :end
Budget: 1000 :end
StartMonth: 10 :end
StartDay: 1 :end
StartHour: 7 :end
StartMinute: 00 :end
ProfitSharing: 50 :end
QuitText: Tired of playing already? :end
:end

//Define the entire site

Site:

Name: Simple Office :end
Description: Welcome to Area 91. :end
:end

Camera:
ViewCenterX: 45 :end
ViewCenterY: 41 :end
ViewAmountBack: 70 :end
ViewAmountUp: 37 :end
:end

// This zone has
// No security included, player will have to add as necessary

Zone:

Name: Entire Office :end
Site: Simple Office :end
Description: The facility currently consists of one zone, compromising the entire available floorspace. :end
//Begin procedural security
HoldsUserAsset: true :end
ProtectWithACL: false :end
WriteDownPasswords: false :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
UpdateAntiVirus: true:end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security
Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false:end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
Re-enforcedWalls: true :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
Network: FLAN :end
ULC: 20 50 :end
LRC: 105 25 :end
:end

// Fender Local Area Network = FLAN

Network:

Name: FLAN :end
NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag

Secrecy:

Name: Fender :end
Level: 64 :end
Category: 0 :end
SecrecyValue: 10000 :end
AttackerValue: 300 :end
InitialBackGroundCheck: Low :end
:end

//Initial DAC group of scientists

DACGroups:
Group: Scientists :end
InitialBackGroundCheck: Low :end
:end

//Asset is the mind control formula

Asset:

Name: Liquid Fluoride Mind Control Formula :end
Description: This formula consists of the mathematical models and detailed chemical properties of the liquid fluoride mind control serum. Due to the highly sensitive nature of this formula, public knowledge of its existence would cause extreme unstability in the local population. Disclosure will result in failure of your mission. :end
IsInstantiated: false :end
HasDac: true :end
Secrecy: Fender :end
DOSMotive: 100 :end
AvailabilityPenalty: 10000 :end
CostList:
Access: *.PUBLIC :end
AccessMode: YNNN :end
Cost: 10000 :end

AttackerMotive: 200 :end
:end //costlist
:end //asset

//Define one asset goal for patrick to read and write the formula

AssetGoal:

Name: Modify Mind Control Formula :end
Description: This goal requires modification of the Liquid Fluoride Mind Control Formula to reflect the latest results of the latest human subject testing. This is a collaborative effort that will fail unless all users who have this goal are able to modify this asset. :end
Shared: true :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 2000 :end
:end //asset goal

//Define user Patrick, cleared to Fender, member of scientists group

User:
Name: Patrick :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 100 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 80 :end
InitialTraining: 70 :end
Happiness: 70 :end
Productivity: 80 :end
Skill: 90 :end
PosIndex: 4 :end

Cost: 1000 :end
Gender: Male :end
UserDescription: Patrick is the inventor of the mind control formula and the chief scientist on the Fender project. Patrick can only modify the formula at the same time that George does. :end
:end //user Patrick

//Define user George, cleared to Fender, member of scientists group

User:
Name: George :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 100 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 50 :end
InitialTraining: 50 :end
Happiness: 80 :end
Productivity: 90 :end
Skill: 90 :end
PosIndex: 2 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: George is a competent scientist, although he is a bit untrustworthy. You may need to keep an eye on him as he may be willing to sell the formula to our enemies. :end
:end //user George

Briefing: Welcome to Area 91. This is Planet Desmid's premiere secret projects research facility. Proceed to your briefing on the game tab.

(PARAGRAPH) You will be responsible for installing and protecting the computer network at this facility.

You have two scientists, Patrick and George, who are working on a highly secret project, code named: Fender. If Fender is compromised, there will be $10,000 in damages and attackers have a 300 motive to attack this project. See the USER tab for more details on these users.

(PARAGRAPH) The Fender project involves a liquid fluoride-based mind control formula. You can find more details about this formula on the ASSET tab. Your goal is to last for thirty days without disclosure of the formula.

(PARAGRAPH) For more information, press 'e' to bring up the encyclopedia. :end

DebriefWin: You win. :end
DebriefLose: You Lose. :end

Conditions:

Condition:
ConditionClass: MinCashOnHand :end
Tagname: MinCashCondition:end
Parameter: 0 :end
Parameter: 1 :end
//Less than $1 min cash on hand. Condition is true if money is zero or less
:end

Condition:
ConditionClass: TimeCondition :end
Tagname: ThirtyDayCondition :end
Parameter: 720 :end //720 hours equals 30 days
:end

Condition:
ConditionClass: TimeCondition :end
Tagname: ThreeDayCondition :end
Parameter: 72 :end
:end

Condition:
ConditionClass: UserFailsGoal :end
Tagname: PatrickFails :end
ConditionText: Patrick :end
SecondConditionText: Modify Mind Control Formula :end
:end

Condition:
ConditionClass: UserFailsGoal :end
Tagname: GeorgeFails :end
ConditionText: George :end
SecondConditionText: Modify Mind Control Formula :end
:end

:end //Conditions

Triggers:

Trigger:

TriggerClass: WinTrigger :end

TriggerName: ThirtyDayTrigger :end

FrequencyInDays: 0.5 :end

TriggerText: You have successfully completed this scenario by satisfying your users' goals for 30 days and avoiding disclosure of the formula. :end

ConditionList: ThirtyDayCondition :end

:end

Trigger:

TriggerClass: LoseTrigger :end

TriggerName: MinCashTrigger :end

FrequencyInDays: 0.5 :end

TriggerText: The mind control formula has been compromised! (PARAGRAPH) (PARAGRAPH) GAME OVER! :end

ConditionList: MinCashCondition :end

:end

Trigger:

TriggerClass: MessageTrigger :end

TriggerName: PatrickNoGoal :end

FrequencyInDays: 1 :end

TriggerText: You have three days to meet the user's goals. :end

ConditionList: PatrickFails OR GeorgeFails :end

:end

Trigger:

TriggerClass: LoseTrigger :end

TriggerName: FailedGoals :end

FrequencyInDays: 1 :end

TriggerText: You have failed to meet the asset goals of your users.

:end

ConditionList: ThreeDayCondition and PatrickFails :end

:end

:end

:EndofFile

B. THREE USERS IN ONE ZONE SCENARIO

// Area 91 small fully playable scenario. This scenario will have three users,two with a //shared goal.

// The player will need to provide the proper components to allow the users to reach their //goal.

```
Organization:

        Name: Desmid_Planetary_Forces           :end
        Title: Area 91 Simple Scenario 1    :end
        StartMoney: 30000   :end
        Budget: 1000        :end
        StartMonth: 10              :end
        StartDay: 1         :end
        StartHour: 7        :end
        StartMinute: 00             :end
        ProfitSharing: 50   :end
        QuitText: Thanks for Playing. Press 'L' to see your results log.    :end
:end

//Define the entire site

Site:
        Name: Simple Office         :end
        Description: Welcome to Area 91. :end
:end

OPTIONS:
UseScenarioCatalogItems: Yes        :end
:end

Camera:
        ViewCenterX:                45      :end
        ViewCenterY:                41      :end
        ViewAmountBack:     70      :end
        ViewAmountUp:               37      :end
:end


// This zone has
// No security included, player will have to add as necessary

Zone:
        Name: Entire Office   :end
```

Site: Simple Office :end
Description: The facility currently consists of one zone, compromising the entire available floorspace. :end

//Begin procedural security
HoldsUserAsset: true :end
ProtectWithACL: false :end
WriteDownPasswords: false :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
UpdateAntiVirus: true:end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: false :end

//End procedural security
Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false:end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: true :end
KeyLockonDoor: false :end
CipherLockonDoor: false :end
ExpensiveIrisScanner: false :end
ModerateIrisScanner: false :end
Badges: false :end
Secrecy: Fender :end
Network: FLAN :end
ULC: 20 50 :end
LRC: 105 25 :end
:end

```
// Fender Local Area Network = FLAN

Network:
        Name: FLAN  :end
        NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag

Secrecy:
        Name: Fender :end
        Level: 64       :end
        Category: 0     :end
        SecrecyValue: 10000  :end
        AttackerValue: 600    :end
        InitialBackGroundCheck: High        :end
:end

//Initial DAC group of scientists

DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:     Low    :end
:end

//Asset is the mind control formula

Asset:
        Name: Liquid Fluoride Mind Control Formula        :end
        Description: This formula consists of the mathematical models and
detailed chemical properties of the liquid fluoride mind control serum. Due to the highly
sensitive nature of this formula, public knowledge of its existence would cause extreme
unstability in the local population. Disclosure will result in failure of your mission.   :end

        IsInstantiated: false    :end
        HasDac: true            :end
        Secrecy: Fender                 :end
        DOSMotive: 100                  :end
        AvailabilityPenalty:   10000  :end
        CostList:
                Access: *.PUBLIC    :end
                AccessMode: YNNN  :end
                Cost: 10000    :end
                AttackerMotive: 200  :end
```

:end //costlist
:end //asset

Asset:
Name: Soda Fund Account :end
Description: The facility operates a a small snack bar and soda machine area. This asset is a bank ledger that tracks the daily income and expenses of the soda fund. If this account gets disclosed, an enemy could determine how many candy bars the users eat and thus judge their overall weight condition. :end

IsInstantiated: false :end
HasDAC: false :end
AvailabilityPenalty: 25 :end
:end

//Define one asset goal for patrick to read and write the formula

AssetGoal:

Name: Modify Mind Control Formula :end
Description: This goal requires modification of the Liquid Fluoride Mind Control Formula to reflect the latest results of the latest human subject testing. This is a collaborative effort that will fail unless all users who have this goal are able to modify this asset. :end
Shared: true :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 2000 :end
:end //asset goal

AssetGoal:
Name: Keep Track of Snack Bar Funds :end
Description: This goal requires modification of the soda fund account. Users with this goal are responsible for running the snack bar and need to know the current funds available so that they may keep the area stocked. :end
Asset:
Name: Soda Fund Account :end
AccessMode: YYXX :end
:end
AvailabilityCostPenalty: 100 :end
:end

```
//Define user Patrick, cleared to Fender, member of scientists group

User:
        Name: Patrick :end
        SecrecyClearance: Fender      :end
        DACGroups:
                Public  :end
                SCIENTISTS  :end
        :end //DAC groups
        DefaultDAC: SCIENTISTS   :end
        AssetGoal:
                AssetGoalName: Modify Mind Control Formula :end
                TargetUsage:  100     :end
                Happiness:    100     :end
                Productivity:  100    :end
        :end //asset goal
        Trustworthiness: 95   :end
        InitialTraining: 95      :end
        Happiness:    95      :end
        Productivity:  95     :end
        Skill:        95      :end
        PosIndex:     4       :end
        Cost:         6000    :end
        Gender:       Male            :end
        UserDescription: Patrick is the inventor of the mind control formula and
the chief scientist on the Fender project.  Patrick can only modify the formula at the same
time that George does.          :end

:end //user Patrick

//Define user George, cleared to Fender, member of scientists group

User:
        Name: George :end
        SecrecyClearance: Fender      :end
        DACGroups:
                Public  :end
                SCIENTISTS  :end
        :end //DAC groups
        DefaultDAC: SCIENTISTS   :end
        AssetGoal:
                AssetGoalName: Modify Mind Control Formula :end
                TargetUsage:  100     :end
                Happiness:    100     :end
```

Productivity: 100 :end
:end //asset goal
Trustworthiness: 96 :end
InitialTraining: 96 :end
Happiness: 96 :end
Productivity: 96 :end
Skill: 96 :end
PosIndex: 2 :end
Cost: 3000 :end
Gender: Male :end
UserDescription: George is Patrick's lab assistant. He is highly skilled, and Patrick considers him to be his right hand man. :end
:end //user George

//Define user Howie, no clearance with a goal to modify the soda fund account

User:
Name: Howie :end
AssetGoal:
AssetGoalName: Keep Track of Snack Bar Funds :end
TargetUsage: 100 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 50 :end
InitialTraining: 50 :end
Happiness: 90 :end
Productivity: 90 :end
Skill: 50 :end
PosIndex: 8 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: Howie is a newly commissioned officer who has been given the tremendous responsibility of running the snack bar. :end
:end //user Howie

//Officer Dan: Security Guard

User:
Name: Officer Dan :end
Dept: Security :end
DACGroups:
Public :end
:end
Trustworthiness: 100 :end

InitialTraining: 100 :end
DaysTillAvailable: 0 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 12 :end
Cost: 1200 :end
Gender: Male :end
UserDescription: Dan likes donuts. :end
:end

Component:
Name: Blato Desktop Select :end
IsTemplate: true :end
Description: Packed with applications, memory and disk :end
AssetProtection: true :end
HW: Blato Desktop Select :end
Cost: 1700 :end
Resale: 200 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Desktop :end
:end

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

Component:
Name: Secure Shade Desktop:end
IsTemplate: true :end
Description: Similar to the Blato Desktop, but includes the Secure Shade OS. :end
AssetProtection: true :end
HW: Blato Desktop Select :end

```
            Cost: 2000              :end
            Resale: 500             :end
            Maintenance: 100        :end
            Availability: 99        :end
            OS: Secure shade Desktop    :end
        :end
```

Briefing: Welcome to Area 91. This is Planet Desmid's premiere secret projects research facility. Proceed to your briefing on the game tab.

(PARAGRAPH) You will be responsible for installing and protecting the computer network at this facility.You have two scientists, Patrick and George, who are working on a highly secret project, code named: Fender. If Fender is compromised, there will be $10,000 in damages and attackers have a 600 motive to attack this project. See the USER tab for more details on these users.

(PARAGRAPH) The Fender project involves a liquid fluoride-based mind control formula. You can find more details about this formula on the ASSET tab. Your main goal is to last for thirty days without disclosure of this formula.

(PARAGRAPH) Your third user, Howie, is responsible for maintaining the facility's snack bar. The scientists rely on the availability of this snack bar, as they are not allowed to bring in food from the outside, neither can they leave for lunch. Without Howie, they would starve.

(PARAGRAPH) For more information, press 'e' to bring up the encyclopedia. :end

```
            DebriefWin:  You win.  :end
            DebriefLose: You Lose.  :end

        Conditions:
            Condition:
                ConditionClass: MinCashOnHand    :end
                Tagname: MinCashCondition:end
                Parameter: 0   :end
                Parameter: 1   :end
                //Less than $1 min cash on hand. Condition is true if money is zero
or less
            :end

            Condition:
                ConditionClass: TimeCondition       :end
                Tagname: ThirtyDayCondition         :end
                Parameter: 720          :end    //720 hours equals 30 days
            :end

        :end //Conditions
```

Triggers:
Trigger:
TriggerClass: WinTrigger :end
TriggerName: ThirtyDayTrigger :end
FrequencyInDays: 0.5 :end
TriggerText: You have successfully completed this scenario by satisfying your users' goals for 30 days and avoiding disclosure of the formula. :end
ConditionList: ThirtyDayCondition :end
:end

Trigger:
TriggerClass: LoseTrigger :end
TriggerName: MinCashTrigger :end
FrequencyInDays: 0.5 :end
TriggerText: The mind control formula has been compromised! (PARAGRAPH) (PARAGRAPH) GAME OVER! :end
ConditionList: MinCashCondition :end
:end
:end

:EndofFile

C. THREE USERS TWO ZONES

// Area 91 small fully playable scenario. This scenario will have three users,two with a //shared goal.
// The player will need to provide the proper components to allow the users to reach their //goal.
// This scenario tests having an uncleared user with a high motive to get into a high value //zone.

Organization:
Name: Desmid_Planetary_Forces :end
Title: Area 91 Simple Scenario 1 :end
StartMoney: 30000 :end
Budget: 1000 :end
StartMonth: 10 :end
StartDay: 1 :end
StartHour: 7 :end
StartMinute: 00 :end
ProfitSharing: 50 :end
QuitText: Thanks for Playing. Press 'L' to see your results log. :end
:end

```
//Define the entire site
Site:
        Name: Simple Office             :end
        Description: Welcome to Area 91. :end
:end

Camera:
        ViewCenterX:                    45      :end
        ViewCenterY:                    41      :end
        ViewAmountBack:     70          :end
        ViewAmountUp:                   37      :end
:end

// This zone has
// No security included, player will have to add as necessary

Zone:
        Name: Entire Office     :end
        Site: Simple Office             :end
        Description: The facility currently consists of two zones, one compromising the entire available floorspace and the other a Fender cleared zone. :end

        //Begin procedural security
        HoldsUserAsset: true    :end
        ProtectWithACL: false           :end
        WriteDownPasswords: false       :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
        UpdateAntiVirus: true:end
        ApplyPatches: true      :end
        LeaveMachinesOn: true           :end
        NoPhysicalModifications: true           :end
        UserBackup: false       :end

        //End procedural security
        Receptionist: false     :end
        GuardatDoor: false      :end
        PatrollingGuard: false:end
```

ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
Re-enforcedWalls: true :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
ULC: 20 50 :end
LRC: 105 25 :end
:end

Zone:
Name: Fender Zone :end
Site: Simple Office :end
Description: The facility currently consists of two zones, one compromising the entire available floorspace and the other a Fender cleared zone. :end

//Begin procedural security
HoldsUserAsset: true :end
ProtectWithACL: false :end
WriteDownPasswords: false :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
UpdateAntiVirus: true:end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security
Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false:end

```
        ProhibitMedia: false   :end
        ProhibitPhoneDevices: false  :end
        ExpensivePerimeterAlarms: false      :end
        Re-enforcedWalls: true         :end
        SurveillanceCameras: true :end
        PermitEscortedVisitors: false  :end
        VisualPeopleInspection: false  :end
        XrayPackages: true    :end
        KeyLockonDoor: false         :end
        CipherLockonDoor: false      :end
        ExpensiveIrisScanner: false  :end
        ModerateIrisScanner: false    :end
        Badges: false  :end
        Secrecy: Fender        :end
        Network: FLAN        :end
        ULC:   49   39 :end
        LRC:  68  26   :end
:end

// Fender Local Area Network = FLAN
Network:
        Name: FLAN  :end
        NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag

Secrecy:
        Name: Fender :end
        Level: 64       :end
        Category: 0    :end
        SecrecyValue: 10000  :end
        AttackerValue: 600    :end
        InitialBackGroundCheck: High        :end
:end

//Initial DAC group of scientists

DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:      Low    :end
:end

//Asset is the mind control formula
```

Asset:

Name: Liquid Fluoride Mind Control Formula :end

Description: This formula consists of the mathematical models and detailed chemical properties of the liquid fluoride mind control serum. Due to the highly sensitive nature of this formula, public knowledge of its existence would cause extreme unstability in the local population. Disclosure will result in failure of your mission. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Fender :end
DOSMotive: 100 :end
AvailabilityPenalty: 10000 :end
CostList:
Access: *.PUBLIC :end
AccessMode: YNNN :end
Cost: 10000 :end
AttackerMotive: 200 :end
:end //costlist
:end //asset

Asset:

Name: Soda Fund Account :end

Description: The facility operates a a small snack bar and soda machine area. This asset is a bank ledger that tracks the daily income and expenses of the soda fund. If this account gets disclosed, an enemy could determine how many candy bars the users eat and thus judge their overall weight condition. :end

IsInstantiated: false :end
HasDAC: false :end
AvailabilityPenalty: 25 :end
:end

//Define one asset goal for patrick to read and write the formula

AssetGoal:

Name: Modify Mind Control Formula :end

Description: This goal requires modification of the Liquid Fluoride Mind Control Formula to reflect the latest results of the latest human subject testing. This is a collaborative effort that will fail unless all users who have this goal are able to modify this asset. :end

Shared: true :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end

:end //asset list
AvailabilityCostPenalty: 2000 :end
:end //asset goal

AssetGoal:
Name: Keep Track of Snack Bar Funds :end
Description: This goal requires modification of the soda fund account. Users with this goal are responsible for running the snack bar and need to know the current funds available so that they may keep the area stocked. :end

Asset:
Name: Soda Fund Account :end
AccessMode: YYXX :end
:end
AvailabilityCostPenalty: 100 :end
:end

//Define user Patrick, cleared to Fender, member of scientists group

User:
Name: Patrick :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 100 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 95 :end
InitialTraining: 95 :end
Happiness: 95 :end
Productivity: 95 :end
Skill: 95 :end
PosIndex: 4 :end
Cost: 6000 :end
Gender: Male :end
UserDescription: Patrick is the inventor of the mind control formula and the chief scientist on the Fender project. Patrick can only modify the formula at the same time that George does. :end

```
:end //user Patrick

//Define user George, cleared to Fender, member of scientists group

User:
        Name: George:end
        SecrecyClearance: Fender      :end
        DACGroups:
                Public  :end
                SCIENTISTS  :end
        :end //DAC groups
        DefaultDAC: SCIENTISTS   :end
        AssetGoal:
                AssetGoalName: Modify Mind Control Formula :end
                TargetUsage:  100     :end
                Happiness:    100     :end
                Productivity:  100    :end
        :end //asset goal
        Trustworthiness: 96   :end
        InitialTraining: 96     :end
        Happiness:    96      :end
        Productivity:  96     :end
        Skill:        96      :end
        PosIndex:     2       :end
        Cost:         3000    :end
        Gender:       Male            :end
        UserDescription: George is Patrick's lab assistant. He is highly skilled, and
Patrick considers him to be his right hand man.       :end

:end //user George

//Define user Howie, no clearance with a goal to modify the soda fund account

User:
        Name: Howie  :end
        AssetGoal:
                AssetGoalName: Keep Track of Snack Bar Funds :end
                TargetUsage:  100     :end
                Happiness:    100     :end
                Productivity:  100    :end
        :end //asset goal
        Trustworthiness: 50   :end
        InitialTraining: 50     :end
        Happiness:    90      :end
        Productivity:  90     :end
```

Skill: 50 :end
PosIndex: 8 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: Howie is a newly commissioned officer who has been given the tremendous responsibility of running the snack bar. :end

:end //user Howie

//Officer Dan: Security Guard

User:
Name: Officer Dan :end
Dept: Security :end
DACGroups:
Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
DaysTillAvailable: 0 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 12 :end
Cost: 1200 :end
Gender: Male :end
UserDescription: Dan likes donuts. :end
:end

Briefing: Welcome to Area 91. This is Planet Desmid's premiere secret projects research facility. Proceed to your briefing on the game tab.

(PARAGRAPH) You will be responsible for installing and protecting the computer network at this facility.You have two scientists, Patrick and George, who are working on a highly secret project, code named: Fender. If Fender is compromised, there will be $10,000 in damages and attackers have a 600 motive to attack this project. See the USER tab for more details on these users.

(PARAGRAPH) The Fender project involves a liquid fluoride-based mind control formula. You can find more details about this formula on the ASSET tab. Your main goal is to last for thirty days without disclosure of this formula.

(PARAGRAPH) Your third user, Howie, is responsible for maintaining the facility's snack bar. The scientists rely on the availability of this snack bar, as they are not allowed to bring in food from the outside, neither can they leave for lunch. Without Howie, they would starve.

(PARAGRAPH) For more information press 'e' to bring up the encyclopedia. :end

```
        DebriefWin:  You win.  :end
        DebriefLose: You Lose.  :end

    Conditions:
        Condition:
            ConditionClass: MinCashOnHand    :end
            Tagname: MinCashCondition:end
            Parameter: 0   :end
            Parameter: 1   :end
            //Less than $1 min cash on hand. Condition is true if money is zero
or less
        :end

        Condition:
            ConditionClass: TimeCondition       :end
            Tagname: ThirtyDayCondition         :end
            Parameter: 720          :end    //720 hours equals 30 days
        :end

    :end //Conditions

    Triggers:
        Trigger:
            TriggerClass: WinTrigger     :end
            TriggerName: ThirtyDayTrigger       :end
            FrequencyInDays: 0.5        :end
            TriggerText: You have successfully completed this scenario by
satisfying your users' goals for 30 days and avoiding disclosure of the formula.     :end

            ConditionList:  ThirtyDayCondition :end
        :end

        Trigger:
            TriggerClass: LoseTrigger    :end
            TriggerName: MinCashTrigger         :end
            FrequencyInDays: 0.5        :end
            TriggerText: The mind control formula has been compromised!
(PARAGRAPH) (PARAGRAPH) GAME OVER!   :end

            ConditionList: MinCashCondition    :end
        :end
    :end

    :EndofFile
```

D. FOUR USERS TWO ZONES SCENARIO

// Area 91 small fully playable scenario. This scenario will have four users,two with a shared goal.

// The player will need to provide the proper components to allow the users to reach their goal.

// This scenario tests having an uncleared user with a medium motive to get into a medium valued asset.

```
Organization:
        Name: Desmid_Planetary_Forces           :end
        Title: Area 91 Simple Scenario 1    :end
        StartMoney: 30000   :end
        Budget: 1000        :end
        StartMonth: 10              :end
        StartDay: 1         :end
        StartHour: 7        :end
        StartMinute: 00             :end
        ProfitSharing: 50   :end
        QuitText: Thanks for Playing. Press 'L' to see your results log.    :end
:end

OPTIONS:
UseScenarioCatalogItems: Yes    :end
:end

//Define the entire site

Site:
        Name: Simple Office         :end
        Description: Welcome to Area 91. :end
:end

Camera:
        ViewCenterX:            45      :end
        ViewCenterY:            41      :end
        ViewAmountBack:  70     :end
        ViewAmountUp:           37      :end
:end

// This zone has
// No security included, player will have to add as necessary
```

Zone:

Name: Entire Office :end
Site: Simple Office :end
Description: The facility currently consists of two zones, one compromising the entire available floorspace and the other a Fender cleared zone. :end

//Begin procedural security
HoldsUserAsset: true :end
ProtectWithACL: false :end
WriteDownPasswords: false :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
UpdateAntiVirus: true:end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security
Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false:end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
Re-enforcedWalls: true :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
ULC: 20 50 :end
LRC: 105 25 :end
:end

Zone:

Name: Fender Zone :end
Site: Simple Office :end
Description: The facility currently consists of two zones, one compromising the entire available floorspace and the other a Fender cleared zone. :end

//Begin procedural security
HoldsUserAsset: true :end
ProtectWithACL: true:end
WriteDownPasswords: false :end
LockorLogoff: true :end
PasswordLength: long:end
PasswordCharacterSet: complex :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseofModems: true :end
NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: true:end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security

Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false:end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: true :end
XrayPackages: true :end
KeyLockonDoor: true:end
CipherLockonDoor: true :end
ExpensiveIrisScanner: true :end
ModerateIrisScanner: false :end
Badges: true :end
Secrecy: Fender :end
PermittedUsers: *.Scientists :end
Network: FLAN :end

```
        ULC:   49   39 :end
        LRC:  68  26   :end
:end

// Fender Local Area Network = FLAN
Network:
        Name: FLAN  :end
        NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag

Secrecy:
        Name: Fender :end
        Level: 64       :end
        Category: 0     :end
        SecrecyValue: 10000  :end
        AttackerValue: 600    :end
        InitialBackGroundCheck: High         :end
:end

Secrecy:
        Name: Secret  :end
        Level: 32       :end
        Category: 0     :end
        SecrecyValue: 5000    :end
        AttackerValue: 300    :end
        InitialBackgroundCheck: High :end
:end

//Initial DAC group of scientists

DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:      Low    :end
:end

//Asset is the mind control formula

Asset:
        Name: Liquid Fluoride Mind Control Formula         :end
        Description: This formula consists of the mathematical models and
detailed chemical properties of the liquid fluoride mind control serum. Due to the highly
sensitive nature of this formula, public knowledge of its existence would cause extreme
unstability in the local population. Disclosure will result in failure of your mission.   :end
```

IsInstantiated: true :end
HasDac: true :end
Secrecy: Fender :end
DOSMotive: 100 :end
AvailabilityPenalty: 10000 :end
AccessList:
*.Scientists YYNN
:end //Accesslist
CostList:
Access: *.PUBLIC :end
AccessMode: YNNN :end
Cost: 10000 :end
AttackerMotive: 200 :end
:end //costlist
:end //asset

Asset:
Name: Soda Fund Account :end
Description: The facility operates a a small snack bar and soda machine area. This asset is a bank ledger that tracks the daily income and expenses of the soda fund. If this account gets disclosed, an enemy could determine how many candy bars the users eat and thus judge their overall weight condition. :end

IsInstantiated: false :end
HasDAC: false :end
AvailabilityPenalty: 25 :end
:end

Asset:
Name: Research Database :end
Description: This asset encompasses the ongoing research efforts of the scientists as they work on various projects at the Secret level and below. :end

IsInstantiated: false :end
HasDAC: True :end
Secrecy: Secret :end
DosMotive: 100 :end
AvailabilityPenalty: 5000 :end
CostList:
Access: *.PUBLIC :end
AccessMode: YNNN :end
Cost: 5000 :end
AttackerMotive: 123 :end
:end

:end

//Define one asset goal for patrick to read and write the formula

AssetGoal:
Name: Modify Mind Control Formula :end
Description: This goal requires modification of the Liquid Fluoride Mind Control Formula to reflect the latest results of the latest human subject testing. This is a collaborative effort that will fail unless all users who have this goal are able to modify this asset. :end

Shared: true :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 2000 :end

:end //asset goal

AssetGoal:
Name: Keep Track of Snack Bar Funds :end
Description: This goal requires modification of the soda fund account. Users with this goal are responsible for running the snack bar and need to know the current funds available so that they may keep the area stocked. :end

Asset:
Name: Soda Fund Account :end
AccessMode: YYXX :end
:end
AvailabilityCostPenalty: 100 :end
:end

AssetGoal:
Name: Work on the Research Database :end
Description: This goal requires modification of the Research Database asset. Users with this goal are responsible for the ongoing daily research at the facility.
:end

Asset:
Name: Research Database :end
AccessMode: YYXX :end
:end
AvailabilityCostPenalty: 200 :end
:end

```
//Define user Patrick, cleared to Fender, member of scientists group

User:
        Name: Patrick :end
        SecrecyClearance: Fender      :end
        DACGroups:
                Public  :end
                SCIENTISTS  :end
        :end //DAC groups
        DefaultDAC: SCIENTISTS   :end
        AssetGoal:
                AssetGoalName: Modify Mind Control Formula :end
                TargetUsage:  100     :end
                Happiness:    100     :end
                Productivity:  100    :end
        :end //asset goal
        Trustworthiness: 95   :end
        InitialTraining: 95      :end
        Happiness:     95       :end
        Productivity:  95       :end
        Skill:         95       :end
        PosIndex:      4        :end
        Cost:          6000     :end
        Gender:        Male             :end
        UserDescription: Patrick is the inventor of the mind control formula and
the chief scientist on the Fender project.  Patrick can only modify the formula at the same
time that George does.          :end

:end //user Patrick

//Define user Stanley, cleared to Secret, member of scientists group

User:
        Name: Stanley:end
        SecrecyClearance: Secret      :end
        AssetGoal:
                AssetGoalName: Work on the Research Database :end
                TargetUsage:  100     :end
                Happiness:    100     :end
                Productivity:  100    :end
        :end //asset goal
        Trustworthiness: 95   :end
        InitialTraining: 95      :end
        Happiness:     95       :end
```

Productivity: 95 :end
Skill: 95 :end
PosIndex: 9 :end
Cost: 6000 :end
Gender: Male :end
UserDescription: Stanley is a mid-level scientist. He has been warned to keep an eye on Howie. :end

:end //user Stanley

//Define user George, cleared to Fender, member of scientists group

User:
Name: George :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 100 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 96 :end
InitialTraining: 96 :end
Happiness: 96 :end
Productivity: 96 :end
Skill: 96 :end
PosIndex: 2 :end
Cost: 3000 :end
Gender: Male :end
UserDescription: George is Patrick's lab assistant. He is highly skilled, and Patrick considers him to be his right hand man. :end

:end //user George

//Define user Howie, no clearance with a goal to modify the soda fund account

User:
Name: Howie :end
AssetGoal:
AssetGoalName: Keep Track of Snack Bar Funds :end

TargetUsage: 100 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 50 :end
InitialTraining: 50 :end
Happiness: 90 :end
Productivity: 90 :end
Skill: 50 :end
PosIndex: 8 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: Howie is a newly commissioned officer who has been given the tremendous responsibility of running the snack bar. :end

:end //user Howie

//Officer Dan: Security Guard

User:
Name: Officer Dan :end
Dept: Security :end
DACGroups:
Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
DaysTillAvailable: 0 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 12 :end
Cost: 1200 :end
Gender: Male :end
UserDescription: Dan likes donuts. :end
:end

Component:
Name: Patrick's Work PC :end
IsTemplate: false :end
AssetProtection: True :end
HW: Trusted Targo Worksaver :end
Static: false :end
Availability: 95 :end
Resale: 200 :end

```
    OS: Populos V9 Desktop :end
    EnforcePasswordPolicy: true :end
    BrowserSettings: Strict :end
    EmailSettings: Strict :end
    UpdateAntivirus: Regular :end
    User: Patrick :end
    PosIndex: 4 :end
    Assets: Liquid Fluoride Mind Control Formula :end
    AccessListLocal: Patrick :end
    AccessListLocal: *.Scientists :end
    AccessListRemote: Patrick :end
    AccessListRemote: Howie :end
    AccessListRemote: *.Scientists :end
    Network:
        Name: FLAN :end
        AccessList: *.Scientists :end AccessMode: YYNN :end
    :end // of network description
    ComponentProceduralSettings:
    ProtectWithACL: true :end
    LockorLogoff: true :end
    PasswordLength: Long :end
    PasswordCharacterSet: Complex :end
    PasswordChangeFrequency: two :end
    NoEmailAttachmentExecute: true :end
    ApplyPatches: true :end
    LeaveMachinesOn: true :end
    NoPhysicalModifications: true :end
    HoldsUserAsset: true :end
    :end // ComponentProceduralSettings
:end //  Component

Component:
    Name: George's Work PC :end
    IsTemplate: false :end
    AssetProtection: True :end
    HW: Trusted Targo Worksaver :end
    Static: false :end
    Availability: 95 :end
    Resale: 200 :end
    OS: Populos V9 Desktop :end
    EnforcePasswordPolicy: true :end
    BrowserSettings: Strict :end
    EmailSettings: Strict :end
    UpdateAntivirus: Regular :end
    User: George :end
```

```
    PosIndex: 2 :end
    AccessListLocal: George :end
    AccessListRemote: George :end
    Network:
      Name: FLAN :end
      AccessList: *.Scientists :end AccessMode: YYNN :end
    :end // of network description
    ComponentProceduralSettings:
    ProtectWithACL: true :end
    LockorLogoff: true :end
    PasswordLength: Long :end
    PasswordCharacterSet: Complex :end
    PasswordChangeFrequency: two :end
    NoEmailAttachmentExecute: true :end
    ApplyPatches: true :end
    LeaveMachinesOn: true :end
    NoPhysicalModifications: true :end
    HoldsUserAsset: true :end
    :end // ComponentProceduralSettings
:end //  Component

//Define Items to be used as the component catalog

Component:
        Name:  Blato Desktop Select :end
        IsTemplate:     true :end
        Description: Packed with applications, memory and disk :end
        AssetProtection:        true :end
        HW:  Blato Desktop Select :end
        Cost: 1700 :end
        Resale: 200 :end
        Maintenance: 100 :end
        Availability: 99 :end
        OS:  Populos V9 Desktop      :end
:end

Component:
        Name: Secure Shade Desktop:end
        IsTemplate: true        :end
        Description: Similar to the Blato Desktop, but includes the Secure Shade
OS.     :end
        AssetProtection: true  :end
        HW: Blato Desktop Select     :end
        Cost: 5000              :end
        Resale: 500             :end
```

```
            Maintenance: 100      :end
            Availability: 99      :end
            OS: Green Shade Core      :end
        :end
```

Briefing: Welcome to Area 91. This is Planet Desmid's premiere secret projects research facility. Proceed to your briefing on the game tab.

(PARAGRAPH) You will be responsible for installing and protecting the computer network at this facility. You have two scientists,Patrick and George, who are working on a highly secret project, code named: Fender. If Fender is compromised, there will be $10,000 in damages and attackers have a 600 motive to attack this project. See the USER tab for more details on these users.

(PARAGRAPH) The Fender project involves a liquid fluoride-based mind control formula. You can find more details about this formula on the ASSET tab. Your main goal is to last for thirty days without disclosure of this formula.

(PARAGRAPH) Your third user, Howie, is responsible for maintaining the facility's snack bar. The scientists rely on the availability of this snack bar, as they are not allowed to bring in food from the outside, neither can they leave for lunch. Without Howie, they would starve.Your fourth user, Stanley, isn't cleared to Fender, but requires access to a Secret project. Meet his goal but keep Howie from accessing it.

(PARAGRAPH) For more information press 'e' to bring up the encyclopedia. :end

```
            DebriefWin:  You win.  :end

            DebriefLose: You Lose.  :end

        Conditions:
            Condition:
                ConditionClass: MinCashOnHand    :end
                Tagname: MinCashCondition:end
                Parameter: 0   :end
                Parameter: 1   :end
                //Less than $1 min cash on hand. Condition is true if money is zero
or less
            :end

            Condition:
                ConditionClass: TimeCondition      :end
                Tagname: ThirtyDayCondition        :end
                Parameter: 720         :end    //720 hours equals 30 days
            :end

        :end //Conditions
```

Triggers:
Trigger:
TriggerClass: WinTrigger :end
TriggerName: ThirtyDayTrigger :end
FrequencyInDays: 0.5 :end
TriggerText: You have successfully completed this scenario by satisfying your users' goals for 30 days and avoiding disclosure of the formula. :end
ConditionList: ThirtyDayCondition :end
:end

Trigger:
TriggerClass: LoseTrigger :end
TriggerName: MinCashTrigger :end
FrequencyInDays: 0.5 :end
TriggerText: The mind control formula has been compromised! (PARAGRAPH) (PARAGRAPH) GAME OVER! :end
ConditionList: MinCashCondition :end
:end
:end

:EndofFile

E. ASSET USAGE CHANGE SCENARIO

// Area 91 small fully playable scenario. This scenario tests the asset usage change trigger.

Organization:
Name: Desmid_Planetary_Forces :end
Title: Area 91 Simple Scenario 1 :end
StartMoney: 5000 :end
Budget: 1000 :end
StartMonth: 10 :end
StartDay: 1 :end
StartHour: 7 :end
StartMinute: 00 :end
ProfitSharing: 50 :end
QuitText: Thanks for playing.:end
:end

//Define the entire site

Site:

```
        Name: Simple Office             :end
        Description: Planet Desmid's premiere secret projects research facility
:end
:end

Camera:
        ViewCenterX:                    45      :end
        ViewCenterY:                    41      :end
        ViewAmountBack:     70          :end
        ViewAmountUp:                   37      :end
:end

// This zone puts the whole work center as Fender only
// No security included, player will have to add as necessary

Zone:
        Name: Entire Office    :end
        Site: Simple Office             :end
        //Begin procedural security
        HoldsUserAsset: true  :end
        AccessList: *.SCIENTISTS  :end  AccessMode: YYXX  :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: true:end
        ApplyPatches: true      :end
        LeaveMachinesOn: true           :end
        NoPhysicalModifications: true           :end
        UserBackup: false       :end

        //End procedural security
        Receptionist: false     :end
        GuardatDoor: false      :end
        PatrollingGuard: false:end
        ProhibitMedia: true     :end
        ProhibitPhoneDevices: true    :end
        ExpensivePerimeterAlarms: true        :end
```

```
        Re-enforcedWalls: true          :end
        SurveillanceCameras: true :end
        PermitEscortedVisitors: false  :end
        VisualPeopleInspection: false  :end
        XrayPackages: true     :end
        KeyLockonDoor: true:end
        CipherLockonDoor: true        :end
        ExpensiveIrisScanner: true  :end
        ModerateIrisScanner: false     :end
        Badges: true    :end
        Secrecy: Fender         :end
        PermittedUsers: *.SCIENTISTS        :end
        Network: FLAN         :end
        ULC:   20   50 :end
        LRC:  105  25   :end
:end

// Fender Local Area Network = FLAN

Network:
        Name: FLAN  :end
        NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag

Secrecy:
        Name: Fender :end
        Level: 64        :end
        Category: 0     :end
        SecrecyValue: 10       :end
        AttackerValue: 1        :end
        InitialBackGroundCheck: High         :end
:end

//Initial DAC group of scientists

DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:      High    :end
:end

//Asset is the mind control formula

Asset:
```

Name: Liquid Fluoride Mind Control Formula :end
Description: The mathematical models and detailed chemical properties of the liquid fluoride-based mind control serum. :end

IsInstantiated: false :end
HasDac: true :end
Secrecy: Fender :end
DOSMotive: 100 :end
AvailabilityPenalty: 100 :end
AccessList:
Patrick YYXX
:end //accesslist

:end //asset

//Define one asset goal for patrick to read and write the formula

AssetGoal:
Name: Modify Mind Control Formula :end
Description: Modify the formula that only the Fender scientists should see. :end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 300000 :end
:end //asset goal

//Define user Patrick, cleared to Fender, member of scientists group

User:
Name: Patrick :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 50 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal

Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 4 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: Patrick is the inventor of the mind control formula and the chief scientist on the fluoride project team. :end

:end //user Patrick

Briefing: This is the Change Asset Usage Scenario. See Game tab for more... (PARAGRAPH) This scenario tests using the change asset usage trigger. On day two, Patrick's asset usage should change from 50 to 100. :end

DebriefWin: You win. :end
DebriefLose: You Lose. :end

Conditions:
Condition:
ConditionClass: TimeCondition :end
Tagname: TwoDayCondition :end
Parameter: 48 :end
:end

:end //Conditions

Triggers:
Trigger:
TriggerClass: ChangeAssetUsageTrigger :end
TriggerName: PatrickChangeUsageTrigger :end
FrequencyInDays: 0.5 :end
TriggerText: Patrick :end
SecondTriggerText: Modify Mind Control Formula :end
Parameter: 100 :end
ConditionList: TwoDayCondition :end
:end
:end

:EndofFile

F. CASH CHANGE SCENARIO

// Area 91 small fully playable scenario. This scenario tests the cash change trigger.

```
Organization:
        Name: Desmid_Planetary_Forces           :end
        Title: Area 91 Simple Scenario 1    :end
        StartMoney: 2000    :end
        Budget: 1000        :end
        StartMonth: 10              :end
        StartDay: 1         :end
        StartHour: 7        :end
        StartMinute: 00             :end
        ProfitSharing: 50   :end
        QuitText: Thanks for playing.:end
:end

//Define the entire site

Site:
        Name: Simple Office         :end
        Description: Planet Desmid's premiere secret projects research facility
:end
:end

Camera:
        ViewCenterX:                45      :end
        ViewCenterY:                41      :end
        ViewAmountBack:     70      :end
        ViewAmountUp:               37      :end
:end


// This zone puts the whole work center as Fender only
// No security included, player will have to add as necessary

Zone:
        Name: Entire Office   :end
        Site: Simple Office         :end
        //Begin procedural security
        HoldsUserAsset: true  :end
        AccessList: *.SCIENTISTS  :end  AccessMode: YYXX  :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: true:end
        ApplyPatches: true     :end
        LeaveMachinesOn: true         :end
        NoPhysicalModifications: true         :end
        UserBackup: false      :end
        //End procedural security
        Receptionist: false      :end
        GuardatDoor: false     :end
        PatrollingGuard: false:end
        ProhibitMedia: true    :end
        ProhibitPhoneDevices: true    :end
        ExpensivePerimeterAlarms: true      :end
        Re-enforcedWalls: true         :end
        SurveillanceCameras: true :end
        PermitEscortedVisitors: false  :end
        VisualPeopleInspection: false  :end
        XrayPackages: true     :end
        KeyLockonDoor: true:end
        CipherLockonDoor: true       :end
        ExpensiveIrisScanner: true  :end
        ModerateIrisScanner: false     :end
        Badges: true    :end
        Secrecy: Fender         :end
        PermittedUsers: *.SCIENTISTS       :end
        Network: FLAN         :end
        ULC:   20   50 :end
        LRC:  105  25   :end
:end

// Fender Local Area Network = FLAN

Network:
        Name: FLAN  :end
        NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag
```

```
Secrecy:
        Name: Fender :end
        Level: 64       :end
        Category: 0     :end
        SecrecyValue: 10       :end
        AttackerValue: 1       :end
        InitialBackGroundCheck: High        :end
:end

//Initial DAC group of scientists

DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:     High    :end
:end

//Asset is the mind control formula

Asset:
        Name: Liquid Fluoride Mind Control Formula        :end
        Description: The mathematical models and detailed chemical properties of
the liquid fluoride-based mind control serum.  :end

        IsInstantiated: false    :end
        HasDac: true             :end
        Secrecy: Fender                 :end
        DOSMotive: 100                  :end
        AvailabilityPenalty:   100      :end
        AccessList:
                Patrick YYXX
        :end //accesslist

:end //asset

//Define one asset goal for patrick to read and write the formula

AssetGoal:
        Name: Modify Mind Control Formula         :end
        Description:  Modify the formula that only the Fender scientists should
see.    :end
        Asset:
                Name: Liquid Fluoride Mind Control Formula        :end
                AccessMode: YYXX  :end
        :end //asset list
        AvailabilityCostPenalty: 300000       :end
```

:end //asset goal

//Define user Patrick, cleared to Fender, member of scientists group

User:
Name: Patrick :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 50 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 4 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: Patrick is the inventor of the mind control formula and the chief scientist on the fluoride project team. :end

:end //user Patrick

Briefing: This is the Cash Change Scenario. See Game tab for more... (PARAGRAPH) This scenario tests using the cash change trigger. On day two, the cash should increase by $5000 :end

DebriefWin: You win. :end
DebriefLose: You Lose. :end

Conditions:
Condition:
ConditionClass: TimeCondition :end
Tagname: TwoDayCondition :end
Parameter: 48 :end
:end

```
:end //Conditions

Triggers:
        Trigger:
                TriggerClass: CashTrigger     :end
                TriggerName: ChangeTheCash        :end
                FrequencyInDays: 0.5          :end
                TriggerText: You have been given more money!      :end
                Parameter: 5000         :end
                ConditionList: TwoDayCondition :end
        :end
:end

:EndofFile
```

G. TWO LOSE TRIGGERS SCENARIO

```
// Area 91 small fully playable scenario. This scenario tests the game's ability to have two //of the same type of triggers.
// Two lose triggers are set to go off on different conditions.

Organization:
        Name: Desmid_Planetary_Forces               :end
        Title: Area 91 Simple Scenario 1      :end
        StartMoney: 5000      :end
        Budget: 1000          :end
        StartMonth: 10                :end
        StartDay: 1           :end
        StartHour: 7          :end
        StartMinute: 00               :end
        ProfitSharing: 50     :end
        QuitText: Thanks for playing.:end
:end

//Define the entire site

Site:
        Name: Simple Office           :end
        Description: Planet Desmid's premiere secret projects research facility
:end
:end

Camera:
        ViewCenterX:                45      :end
```

```
        ViewCenterY:                41      :end
        ViewAmountBack:    70       :end
        ViewAmountUp:               37      :end
:end

// This zone puts the whole work center as Fender only
// No security included, player will have to add as necessary

Zone:
        Name: Entire Office   :end
        Site: Simple Office             :end
        //Begin procedural security
        HoldsUserAsset: true  :end
        AccessList: *.SCIENTISTS  :end  AccessMode: YYXX  :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: true:end
        ApplyPatches: true     :end
        LeaveMachinesOn: true         :end
        NoPhysicalModifications: true         :end
        UserBackup: false      :end
        //End procedural security

        Receptionist: false      :end
        GuardatDoor: false     :end
        PatrollingGuard: false:end
        ProhibitMedia: true    :end
        ProhibitPhoneDevices: true    :end
        ExpensivePerimeterAlarms: true      :end
        Re-enforcedWalls: true         :end
        SurveillanceCameras: true :end
        PermitEscortedVisitors: false  :end
        VisualPeopleInspection: false  :end
        XrayPackages: true     :end
        KeyLockonDoor: true:end
        CipherLockonDoor: true       :end
```

```
            ExpensiveIrisScanner: true  :end
            ModerateIrisScanner: false     :end
            Badges: true    :end
            Secrecy: Fender         :end
            PermittedUsers: *.SCIENTISTS        :end
            Network: FLAN         :end
            ULC:   20   50 :end
            LRC:  105  25   :end
        :end

        // Fender Local Area Network = FLAN

        Network:
            Name: FLAN  :end
            NetID: 6.6.6.0 :end
        :end

        //Define the Fender Secrecy Tag

        Secrecy:
            Name: Fender :end
            Level: 64        :end
            Category: 0     :end
            SecrecyValue: 10       :end
            AttackerValue: 1        :end
            InitialBackGroundCheck: High         :end
        :end

        //Initial DAC group of scientists

        DACGroups:
            Group: Scientists        :end
            InitialBackGroundCheck:      High    :end
        :end

        //Asset is the mind control formula

        Asset:
            Name: Liquid Fluoride Mind Control Formula         :end
            Description: The mathematical models and detailed chemical properties of
the liquid fluoride-based mind control serum.  :end

            IsInstantiated: false     :end
            HasDac: true            :end
            Secrecy: Fender                 :end
```

```
        DOSMotive: 100              :end
        AvailabilityPenalty:  100   :end
        AccessList:
            Patrick YYXX
        :end //accesslist

    :end //asset

    //Define one asset goal for patrick to read and write the formula

    AssetGoal:
        Name: Modify Mind Control Formula       :end
        Description:  Modify the formula that only the Fender scientists should
see.    :end
        Asset:
            Name: Liquid Fluoride Mind Control Formula      :end
            AccessMode: YYXX  :end
        :end //asset list
        AvailabilityCostPenalty: 300000     :end
    :end //asset goal

    //Define user Patrick, cleared to Fender, member of scientists group

    User:
        Name: Patrick :end
        SecrecyClearance: Fender    :end
        DACGroups:
            Public  :end
            SCIENTISTS  :end
        :end //DAC groups
        DefaultDAC: SCIENTISTS  :end
        AssetGoal:
            AssetGoalName: Modify Mind Control Formula :end
            TargetUsage:  100   :end
            Happiness:    100   :end
            Productivity:  100  :end
        :end //asset goal
        Trustworthiness: 100  :end
        InitialTraining: 100  :end
        Happiness:    100     :end
        Productivity:  100    :end
        Skill:        100     :end
        PosIndex:     4       :end
        Cost:         1000    :end
        Gender:       Male          :end
```

UserDescription: Patrick is the inventor of the mind control formula and the chief scientist on the fluoride project team. :end

:end //user Patrick

Briefing: This is the Two Lose Triggers Scenario. See Game tab for more... (PARAGRAPH) This scenario tests using two lose triggers. You can fail by either losing all of your money or by lasting for two days. :end

DebriefWin: You win. :end

DebriefLose: You Lose. :end

Conditions:

Condition:

ConditionClass: MinCashOnHand :end

Tagname: MinCashCondition:end

Parameter: 0 :end

Parameter: 1 :end

//Less than $1 min cash on hand. Condition is true if money is zero or less

:end

Condition:

ConditionClass: TimeCondition :end

Tagname: TwoDayCondition :end

Parameter: 48 :end

:end

:end //Conditions

Triggers:

Trigger:

TriggerClass: LoseTrigger :end

TriggerName: TwoDayTrigger :end

FrequencyInDays: 0.5 :end

TriggerText: You have lost the scenario by reaching 2 days.:end

ConditionList: TwoDayCondition :end

:end

Trigger:

TriggerClass: LoseTrigger :end

TriggerName: MinCashTrigger :end

FrequencyInDays: 0.5 :end

TriggerText: You have lost all of your money. (PARAGRAPH) (PARAGRAPH) GAME OVER! :end

```
                ConditionList: MinCashCondition     :end
        :end
:end

:EndofFile
```

H. TWO TRIGGERS AT ONCE SCENARIO

```
// Area 91 small fully playable scenario. This scenario tests the game's ability to have multiple triggers based on the
// same condition. Two triggers will fire at the same time based on a single condition.

Organization:
        Name: Desmid_Planetary_Forces           :end
        Title: Area 91 Simple Scenario 1        :end
        StartMoney: 5000        :end
        Budget: 1000            :end
        StartMonth: 10                  :end
        StartDay: 1             :end
        StartHour: 7            :end
        StartMinute: 00                 :end
        ProfitSharing: 50       :end
        QuitText: Thanks for playing.:end
:end

//Define the entire site

Site:
        Name: Simple Office             :end
        Description: Planet Desmid's premiere secret projects research facility
:end
:end

Camera:
        ViewCenterX:                    45      :end
        ViewCenterY:                    41      :end
        ViewAmountBack:     70          :end
        ViewAmountUp:                   37      :end
:end

// This zone puts the whole work center as Fender only
// No security included, player will have to add as necessary
```

Zone:

Name: Entire Office :end
Site: Simple Office :end
//Begin procedural security
HoldsUserAsset: true :end
AccessList: *.SCIENTISTS :end AccessMode: YYXX :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: true :end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UserBackup: false :end
//End procedural security

Receptionist: false :end
GuardatDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
PermitEscortedVisitors: false :end
VisualPeopleInspection: false :end
XrayPackages: true :end
KeyLockonDoor: true :end
CipherLockonDoor: true :end
ExpensiveIrisScanner: true :end
ModerateIrisScanner: false :end
Badges: true :end
Secrecy: Fender :end
PermittedUsers: *.SCIENTISTS :end
Network: FLAN :end
ULC: 20 50 :end
LRC: 105 25 :end

```
:end

// Fender Local Area Network = FLAN

Network:
        Name: FLAN  :end
        NetID: 6.6.6.0 :end
:end

//Define the Fender Secrecy Tag

Secrecy:
        Name: Fender :end
        Level: 64       :end
        Category: 0     :end
        SecrecyValue: 10       :end
        AttackerValue: 1       :end
        InitialBackGroundCheck: High        :end
:end

//Initial DAC group of scientists

DACGroups:
        Group: Scientists       :end
        InitialBackGroundCheck:      High    :end
:end

Asset:
        Name: Liquid Fluoride Mind Control Formula        :end
        Description: The mathematical models and detailed chemical properties of
the liquid fluoride-based mind control serum.  :end

        IsInstantiated: false    :end
        HasDac: true             :end
        Secrecy: Fender                 :end
        DOSMotive: 100                  :end
        AvailabilityPenalty:   100      :end
        AccessList:
                Patrick YYXX
        :end //accesslist
:end //asset

//Define one asset goal for patrick to read and write the formula

AssetGoal:
```

Name: Modify Mind Control Formula :end
Description: Modify the formula that only the Fender scientists should see.:end
Asset:
Name: Liquid Fluoride Mind Control Formula :end
AccessMode: YYXX :end
:end //asset list
AvailabilityCostPenalty: 300000 :end
:end //asset goal

//Define user Patrick, cleared to Fender, member of scientists group

User:
Name: Patrick :end
SecrecyClearance: Fender :end
DACGroups:
Public :end
SCIENTISTS :end
:end //DAC groups
DefaultDAC: SCIENTISTS :end
AssetGoal:
AssetGoalName: Modify Mind Control Formula :end
TargetUsage: 50 :end
Happiness: 100 :end
Productivity: 100 :end
:end //asset goal
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 100 :end
Productivity: 100 :end
Skill: 100 :end
PosIndex: 4 :end
Cost: 1000 :end
Gender: Male :end
UserDescription: Patrick is the inventor of the mind control formula and the chief scientist on the fluoride project team. :end

:end //user Patrick

Briefing: This is the Two Triggers at One Time Scenario. See Game tab for more... (PARAGRAPH) This scenario tests the game's ability to have multiple triggers occur from the same condition. Using a time condition, after one day a message trigger and a log trigger should go off. :end

DebriefWin: You win. :end

```
        DebriefLose: You Lose.  :end

Conditions:
        Condition:
                ConditionClass: TimeCondition       :end
                Tagname: OneDayCondition  :end
                Parameter: 24  :end
        :end
:end //Conditions

Triggers:
        Trigger:
                TriggerClass: MessageTrigger        :end
                TriggerName: OneDayMessage      :end
                FrequencyInDays: 0.5        :end
                TriggerText: One day has gone by.   :end
                ConditionList: OneDayCondition :end
        :end

        Trigger:
                TriggerClass: LogTrigger    :end
                TriggerName: OneDayLogEntry     :end
                FrequencyInDays: 0.5        :end
                TriggerText: This log entry says that one day has gone by.  :end
                ConditionList: OneDayCondition :end
        :end
:end

:EndofFile
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[ASTD] American Society for Training and Development (2002). Training for the Next Economy: An ASTD State of the Industry Report on Trends in Employer-Provided Training in the United States. Retrieved (June 2004) from the World Wide Web: http://www.astd.org/NR/rdonlyres/1E15A3F3-8908-4E21-B5CC-BCEBE02275D1/0/SOIR2002_Training_summary.pdf

[Brinkley] Brinkley, Donald L. & Schell, Roger R (1995). Concepts and Terminology for Computer Security. Ed. Abrams, Jajodia, and Podell. Los Alamitos: IEEE Computer Society Press.

[Clark] Clark, David R. & Wilson, David R. (1987). A Comparison of Commercial and Military Computer Security Policies.

[CNN] Songini, Marc L. (2000). Hospital Confirms Copying of Patient Files by Hacker. Retrieved (April 2004) from the World Wide Web: http://www.cnn.com/2000/TECH/computing/12/15/hospital.hacker.idg/

[Cox] Cox,, Peter (1999). Security Evaluation: The Common Criteria Certifications. Retrieved (April 2004) from the World Wide Web: http://www.itsecurity.com/papers/border.htm

[Irvine] Irvine, Cynthia E. & Thompson, Michael (2003). Teaching Objectives of a Simulation Game for Computer Security. Naval Postgraduate School Center for Information Systems Security Studies and Research. Retrieved (April 2004) from the World Wide Web: http://cisr.nps.navy.mil/downloads/CyberCiege_WP.pdf

[McLean] McLean, John (1994). Security Models.

[NCSC] Department of Defense Standard (1985). Department of Defense Trusted Computer System Evaluation Criteria. Retrieved (April 2004) from the World Wide Web: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[NIST] Griffith, Richard A. & McGregor, Mac E. (1996) Designing & Operating a Multilevel Security Network Using Standard Commercial Products. Retrieved (April 2004) from the World Wide Web: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper037/sctycon2.pdf

[Rivermind 2002] Rivermind, Inc. & Naval Postgraduate School Center for Information Systems Security Studies and Research (2002). CyberCIEGE: Scenario Format Template.

[Sterne] Sterne, Daniel F. (1991). On the Buzzword "Security Policy".

[USATODAY] Associated Press (2003). Tiny Nevada Hospital Attacked by Russian Hacker. Retrieved (April 2004) from the World Wide Web: http://www.usatoday.com/tech/webguide/internetlife/2003-04-07-hospital-hack_x.htm

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. George Bieber
   OSD
   Washington, DC

4. RADM Joseph Burns
   Fort George Meade, MD

5. Deborah Cooper
   DC Associates, LLC
   Roslyn, VA

6. CDR Daniel L. Currie
   PMW 161
   San Diego, CA

7. LCDR James Downey
   NAVSEA
   Washington, DC

8. Richard Hale
   DISA
   Falls Church, VA

9. LCDR Scott D. Heller
   SPAWAR
   San Diego, CA

10. Wiley Jones
    OSD
    Washington, DC

11. Russell Jones
    N641
    Arlington, VA

12. David Ladd
Microsoft Corporation
Redmond, WA

13. Dr. Carl Landwehr
National Science Foundation
Arlington, VA

14. Steve LaFountain
NSA
Fort Meade, MD

15. Dr. Greg Larson
IDA
Alexandria, VA

16. Ray A. Letteer
Head, Information Assurance, HQMC C4 Directorate
Washington, DC

17. Penny Lehtola
NSA
Fort Meade, MD

18. Ernest Lucier
Federal Aviation Administration
Washington, DC

19. CAPT Sheila McCoy
Headquarters U.S. Navy
Arlington, VA

20. Dr. Ernest McDuffie
National Science Foundation
Arlington, VA

21. Dr. Vic Maconachy
NSA
Fort Meade, MD

22. Doug Maughan
Department of Homeland Security
Washington, DC

23. Dr. John Monastra
Aerospace Corporation
Chantilly, VA

24. John Mildner
SPAWAR
Charleston, SC

25. Marshall Potter
Federal Aviation Administration
Washington, DC

26. Dr. Roger R. Schell
Aesec
Pacific Grove, CA

27. Keith Schwalm
Good Harbor Consulting, LLC
Washington, DC

28. Dr. Ralph Wachter
ONR
Arlington, VA

29. David Wirth
N641
Arlington, VA

30. Daniel Wolf
NSA
Fort Meade, MD

31. CAPT Robert Zellmann
CNO Staff N614
Arlington, VA

32. Dr. Cynthia E. Irvine
Naval Postgraduate School
Monterey, CA

33. Paul C. Clark
Naval Postgraduate School
Monterey, CA

34. Michael F. Thompson
Naval Postgraduate School
Monterey, CA

35. LT Robert LaMore
Naval Postgraduate School
Monterey, CA