A CYBERCIEGE SCENARIO ILLUSTRATING MULTILEVEL SECRECY ISSUES IN AN AIR OPERATIONS CENTER ENVIRONMENT

by

Marc K. Meyer

June 2004

Thesis Co-Advisors:
Cynthia Irvine
Paul C. Clark

Second Reader:
Mike Thompson

Approved for public release; distribution is unlimited
REPORT DOCUMENTATION PAGE

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: A CyberCIEGE Scenario Illustrating Multilevel Secrecy Issues in an Air Operations Center Environment

5. FUNDING NUMBERS

6. AUTHOR(S) Marc K. Meyer

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)
    CyberCIEGE provides an addition to traditional Information Assurance (IA) education in the form of an interactive, entertaining, commercial-grade PC-based computer game. Educational objectives are contained in scenarios that serve to teach particular IA concepts. The details of a scenario are contained in a Scenario Definition File (SDF), which is written in the CyberCIEGE Scenario Definition Language. This language is rich enough to express a range of information security policies and operational data access requirements, resulting in a nearly limitless pool of possible scenarios.

    This thesis developed a playable scenario illustrating confidentiality protection concepts in an open storage environment modeled after an Air Operations Center. Educational goals include physical protection of high value assets and use of strong authentication policies to protect moderate value assets. The major work of this thesis was designing an SDF to reflect a military information security policy and work flow environment contained in the educational goals. The confirmation of the proper operation of selected aspects of the CyberCIEGE game engine, and the assurance that the SDF confronts the player with the security trade-offs occurred through the application of a testing methodology. The creation of detailed solutions and incorrect gameplay examples constitute this testing process.

14. SUBJECT TERMS CyberCIEGE, Information Assurance, IA, Scenario Definition File, SDF, Network Security Training

15. NUMBER OF PAGES 190

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
A CYBERCIEGE SCENARIO ILLUSTRATING MULTILEVEL SECRECY ISSUES IN AN AIR OPERATIONS CENTER ENVIRONMENT

Marc K. Meyer
Captain, United States Air Force
B.S., Norwich University, 1999

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: Marc K. Meyer

Approved by: Cynthia Irvine
Thesis Co-Advisor

Paul C. Clark
Thesis Co-Advisor

Mike Thompson
Second Reader

Peter Denning
Chairman, Department of Computer Science
ABSTRACT

CyberCIEGE provides an addition to traditional Information Assurance (IA) education in the form of an interactive, entertaining, commercial-grade PC-based computer game. Educational objectives are contained in scenarios that serve to teach particular IA concepts. The details of a scenario are contained in a Scenario Definition File (SDF), which is written in the CyberCIEGE Scenario Definition Language. This language is rich enough to express a range of information security policies and operational data access requirements, resulting in a nearly limitless pool of possible scenarios.

This thesis developed a playable scenario illustrating confidentiality protection concepts in an open storage environment modeled after an Air Operations Center. Educational goals include physical protection of high value assets and use of strong authentication policies to protect moderate value assets. The major work of this thesis was designing an SDF to reflect a military information security policy and work flow environment contained in the educational goals. The confirmation of the proper operation of selected aspects of the CyberCIEGE game engine, and the assurance that the SDF confronts the player with the security trade-offs occurred through the application of a testing methodology. The creation of detailed solutions and incorrect gameplay examples constituted this testing process.
# TABLE OF CONTENTS

## I. INTRODUCTION
   - THESIS STATEMENT ................................................................. 1
   - GENERAL BACKGROUND .......................................................... 1
     1. Potential Causes ................................................................. 1
        a. Mainframes to PCs ............................................................. 2
        b. Education in the Past and Present ....................................... 2
     2. Where to Go From Here? ...................................................... 2
   - SCENARIO FOCUS ................................................................. 4
     1. Combat Plans Division ......................................................... 5
     2. Combat Operations Division ............................................... 5
   - THE MECHANICS OF CYBERCIEGE ......................................... 5
   - CHAPTER OVERVIEW .......................................................... 6

## II. SCENARIO DESCRIPTION
   - INTENDED USERS ................................................................. 9
   - EDUCATIONAL GOALS .......................................................... 10
     1. Specific Goals ................................................................. 10
        a. Networks that Exist at Different Levels of Classification Need to be Kept Separate .................................................. 10
        b. The Information at the Highest Level of Classification Needs to Be Given the Most Consideration in Terms of Security .................................................. 11
        c. User Training, Physical Security, and Network Security Need to be Applied Together because Application of One is Ineffective without the Other .................................................. 11
        d. Authentication Controls and Password Policies are a Suitable Defense Mechanism for Some Environments Having Shared Physical Space .................................................. 11
     2. The Scenario Gaming Approach ........................................... 12
   - SCENARIO DEVELOPMENT APPROACH .................................. 12
   - SCENARIO BRIEFING ........................................................... 13
     1. The Briefing ................................................................. 13
        a. Plans Division ................................................................. 14
        b. Intelligence Planning Cell ................................................ 14
        c. Logistics Planning Cell .................................................... 14
        d. Weather Planning Cell ..................................................... 15
        e. ATO Production Cell ........................................................ 15
        f. Current Operations Division ............................................. 15
        g. Your Job ................................................................. 16
   - SCENARIO DETAILS ............................................................ 18
     1. Organization ................................................................. 18
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.</td>
<td>AOC Conceptual Division of Labor</td>
<td>14</td>
</tr>
<tr>
<td>Figure 2.</td>
<td>Workflow in the Plans Division</td>
<td>15</td>
</tr>
<tr>
<td>Figure 3.</td>
<td>Workflow in Current Ops Division</td>
<td>16</td>
</tr>
<tr>
<td>Figure 4.</td>
<td>Hierarchy of Secrecy Classifications</td>
<td>17</td>
</tr>
</tbody>
</table>
LIST OF TABLES

Table 1. Basic Set Results........................................................................................................31
Table 2. Secrecy Label Set Results.........................................................................................31
Table 3. Shared Access Set Results ........................................................................................32
Table 4. Attack Loss Trigger Set Results ..............................................................................33
Table 5. Network Connections Set Results............................................................................33
Table 6. AOC Scenario Development Steps ..........................................................................34
Table 7. Bad Security Choice Scenario Results.....................................................................36
ACKNOWLEDGMENTS

I would like to thank Mike Thompson, Paul Clark and Dr. Cynthia Irvine for their support and guidance in bringing this thesis together.

I would like to thank Rob LaMore for being the best person you could possibly share an office with through these tough times at school. You’ve been a great friend and a great help.

I would really like to thank my wife Brenda for being the greatest support for me during the thesis writing process. You provided me with great insight and put in a lot of time to make this thesis better than it would otherwise have been.
THIS PAGE INTENTIONALLY LEFT BLANK
I. INTRODUCTION

A. THESIS STATEMENT

Currently, computer security education is gaining attention. In addition to traditional education methods, new educational approaches are now of interest. The CyberCIEGE simulation game is one of these alternatives being explored at the Naval Postgraduate School. The purpose of this thesis is to examine the following questions in terms of the CyberCIEGE game:

- Is it possible to develop a scenario about multiple confidentiality levels that is both a playable game and an educational tool? Can such a scenario illustrate the traits and habits of good security conduct?
- Is it possible to write a scenario to test the CyberCIEGE game engine’s ability to properly simulate and react to the conditions of multiple confidentiality levels in an open storage area?

Almost no limit exists to the number of security topics that can be explored in the CyberCIEGE game. The objective of this thesis is to answer as many questions as possible regarding the simulation’s ability to support the scenario described above.

B. GENERAL BACKGROUND

In the evolution and application of computer technology, the computer has evolved from a large, bulky tabulating machine inaccessible to the mass public residing in a government or corporate office back room, into the internet-enabled window to the world sitting on nearly every desktop. Whether advancing the productivity of the modern workplace or not, the computer is here to stay. Unfortunately, an understanding of basic security practices necessary to realize the potential of computers and computer networks completely has yet to make its way to the average computer user.

1. Potential Causes

The following are some factors that may have contributed to this disparity between the current dangers in the cyber world and the average computer users’ awareness of those dangers.
a. **Mainframes to PCs**

The use of shared resource mainframes was an early example of many users sharing one computing environment. This type of sharing created a focus on the security mechanisms for information protection within the system [Ware 1967]. A paradigm shift occurred with the advance of the personal computer. No longer would users have to utilize the same computer to accomplish their work. Everyone could have a personal machine and could secure it in their individual physical spaces. Safeguards within the system were no longer a high priority because the sole user physically secured the computing space and no one else would gain local access to that machine. However, the advance of the Internet into nearly every office and home has made that personal computing space accessible to other users again. Although similar to the Mainframe situation users are not as aware of the privacy and information protection issues.

b. **Education in the Past and Present**

Based on information from the Pew Internet Project Survey conducted in February 2004, broadband Internet connections were available to 55% of all Americans and over 68 million adults utilized at least one of the various types of broadband connections available (DSL, cable modem, etc) [Horrigan 2004]. With so many users joining the cyber community, there has been a renewed effort to educate them about the dangers of malicious activity on the Internet. Television commercials and magazine advertisements utilize keywords such as identity theft and virus attack to sell their products. The average user has heard these words, but still has no real understanding of the danger or protection against it. This lack of understanding contributes to poor security habits in user’s personal lives, which then extends into their work environment, which is then at risk from computer attack.

2. **Where to Go From Here?**

Now that computers have become such a large part of daily life, where should education occur? One notion is to conduct extensive training for users on good security habits in the workplace. If successful, the organization gains a measure of security, and as a side effect, users take the good habits they have learned and apply them at home, broadening the effect of security education.
Education and training, however, is expensive. If they do not understand the risks of computer-based attack, then managers will be unable to justify high costs for computer security implementation and education. A good security posture is difficult to measure because it results in non-activity, i.e., there are no security breaches. This is unlike many of the traditional metrics in business where results are measured by various standards, i.e., units produced, customers serviced, or profit gained. The very essence of a good security posture is that nothing happens, which does not provide management with any metrics to review so that they may gain understanding of the risks. Management must be educated on the risks before it can understand the value of security. Traditional methods of security training and education, however, can be confusing under the best circumstances and outright boring under the worst. These methods, when applied to security, will not capture the attention of management or the basic computer user. An alternative to traditional education is simulation, where the public can see the justification for security mechanisms and policies first hand. As Saunders puts it, “Promoting a better understanding of the information security environment…can be effectively achieved through the use of modeling and simulation” [Saunders 2003].

If modeling and simulation can effectively achieve understanding by allowing people to explore “what if” situations, then allowing them to step into the “drivers’ seat” and have them virtually experience specific scenarios. These experiences then it can serve to punctuate security lessons learned by “hammering home” the effects of security violations in virtual settings. The use of simulation games to illustrate situations is not a new concept and there have been several ventures into this area for the purposes of education. In 1997, the Joint Chiefs of Staff wanted to have a laboratory to teach the principles of “joint doctrine”, i.e., how to coordinate the efforts of several branches of the military into one coordinated effort. The result was the creation of “Joint Force Employment” by OC Incorporated, a Virginia-based defense contractor. The purpose of the game was to illustrate the application of military force from a variety of viewpoints, without having to organize costly “live” exercises involving the various branches of the military. In this manner, various military leaders are able to exercise the principles of “joint doctrine” realistically without having to put real troops into the field [Schuster 2001].
Products released in the area of network attack and computer simulation are described in detail in [Teo 2003], *CyberProtect, Information Security Wargaming System* (ISWS) [Saunders 2003], and *AI Wars: The Awakening* [Nexus 2003]. These projects preceded the CyberCIEGE game, but did not contribute to it directly. Conceived by the Center for Information Systems Security Studies Research (CISR) at the Naval Postgraduate School, commercial video game developer, Rivermind, Inc., was engaged to develop a game engine. CISR has been designated by the National Security Agency as Center of Excellence in Information Assurance and its work has pioneered research in the area of malicious software and system subversion [CISR 2004]. The marriage of Rivermind’s game development knowledge and CISR’s experience researching security principles and policies has led to a portable self-contained laboratory tool that can teach its students through practical exercises without the danger of “real” losses.

C. SCENARIO FOCUS

This thesis is intended to illustrate specific security principles utilizing the CyberCIEGE game. The focus of research was on a very narrow set of principles so that they may be covered in depth in the thesis. This thesis centers on the need for real-time sharing of assets in a networked environment, multiple secrecy levels coexisting in a large open-storage area, and the fulfillment of user goals, which may conflict with security posture and policies. To illustrate these issues in a contemporary setting, this scenario models a scaled-down version of an Air Operations Center (AOC). The purpose of an AOC is to organize and deploy air forces for operations in war or conflict [12AF SOP]. No example of the exact structure of an AOC size or structure exists, as it is a flexible entity that caters itself to the severity of the conflict it is intended to support. There are, however, components of this organization that are always present. Thus the CyberCIEGE scenario addresses a broad AOC-like structure. There are two divisions of labor, Plans and Operations, which will contain units with specific duties within them, called cells, described briefly below.
1. **Combat Plans Division**
   
   This division includes three specialized cells within it:
   
   - Intelligence Planning Cell
   - Logistics Planning Cell
   - Weather Planning Cell
   
   Combat plans cells create their individual deliverables and forward them to the Air Tasking Order (ATO) Production Cell.

2. **Combat Operations Division**
   
   The Combat Operations division in a real AOC has many cells in it to distribute the work of controlling the air war. In this scenario, however, this section is a stand-alone division that abstractly performs all the functions expected from an AOC Combat Ops Division.

D. **THE MECHANICS OF CYBERCIEGE**

   The CyberCIEGE game is comprised of two main parts, a commercial grade graphics engine designed to give the player a true feeling of interacting with his enterprise and an AI engine, which is the driving force of the game. However, before the game even begins, another critical part of the game that sets the stage for the experience of the player is necessary: the scenario. The scenario is the “what I am doing this for?” part of the player experience. It is created by a scenario designer to illustrate specific security situations to the player. The scenario designer crafts the scene by defining and including or not including the following elements as defined by the Scenario Format Template (SFT) [Rivermind 2003]:
   
   - Organization
   - Sites
   - Zones
   - Departments
   - Networks
   - Secrecy Levels
   - Integrity Levels
   - DAC Groups
   - Assets
The player, in the role of IT manager for a corporation, then begins with a set of conditions and makes choices through the interface of the game, adding equipment, hiring IT staff, and adding both physical and procedural security options to the enterprise. The intent of the choices that the player makes is to achieve the stated goal of the scenario which is conveyed to the player through the briefing. At this point, the AI engine becomes a factor, by constantly evaluating the state of the game and creating adversity for the player in the form of attackers or incompetent users. The ability of the player to achieve his goals and the amount of adversity he receives, i.e., how much money is lost due to successful attacks or security violations, is a direct result of how well the player builds up his network to defend against the AI engine. Therefore, it becomes apparent that the initial game settings are critical to the lessons that the player is supposed to learn. The Scenario Definition File (SDF) is the blueprint that the scenario designer constructs to illustrate his intended lesson.

A SDF is written in a definition language unique to this game. Rivermind and CISR together created the syntax for this language. The complete syntax of an SDF is defined in the Scenario Format Template (SFT). The content of the SDF is critical to the learning experience of the player. By including or excluding certain material, it is then possible to tailor an SDF to focus on specific security concepts.

E. CHAPTER OVERVIEW

This thesis will describe the reasons behind and the details of a game scenario illustrating a specific set of information security principles. The organization of the remaining chapters is:
• **Chapter II** – Scenario Description. This chapter will pose the research questions that the scenario devised for this thesis is attempting to answer. It will also present a detailed narrative description of the scenario explaining all the values for the scenario contained in the scenario definition file.

• **Chapter III** – Testing. This chapter will describe the methodology used for testing and the results found.

• **Chapter IV** – Future Work and Conclusions. This chapter will suggest other directions future scenario authors may take with this scenario’s principles and discuss the answers to the posed research questions.
II. SCENARIO DESCRIPTION

A. INTENDED USERS

Every computer user in the military is required to complete a form of basic computer user training, which varies depending on military branch. The Air Force in particular employs the C4 Systems Security Awareness, Training, and Education (SATE) Program. The SATE program has the objective “to train individuals to act or react automatically and responsibly to protect information generated, stored, processed, transferred, or communicated by C4 systems” [AFI 33-204 1994]. Every player of the Air Operations Center (AOC) CyberCIEGE scenario is guaranteed to have had SATE training. By virtue of having had SATE training, they know that it is necessary to protect information at higher classifications more than information at lower classifications, although they do not necessarily know how to implement that security.

This CyberCIEGE scenario specifically targets a group of military personnel who completed basic computer user training and are familiar with computers and network technology in the workplace, but do not possess precise knowledge of its implementation. This target audience does not need to know the protocols necessary for successful network communications or the required firmware versions on network devices. The game engine removes many of the specific technical details. Specific knowledge of Mandatory Access Controls (MAC) and Discretionary Access Control (DAC) concepts are also not required knowledge for these players. The introductory brief for the scenario and definitions in the CyberCIEGE encyclopedia, along with some experience with other CyberCIEGE tutorials provides the players all the needed information for a success when playing this scenario.

The educational benefit of this scenario is greatest for players possessing broad knowledge of security concepts, but lack depth. Players who have very specific security implementation insights are more likely to “solve” the problem quickly and not encounter many of the built in lesson mechanisms. These mechanisms exist to reinforce the impact of specific choices, which highlight the educational goals of the scenario, i.e., what the player is supposed to learn from the game experience.
B. EDUCATIONAL GOALS

The AOC represents a great challenge in the application of computer security. It is an environment whose requirements include flexible information access and support of many different cells which need to share information with each other in real-time. While this is already a complicated requirement, shared information is not all classified at the same level, and the personnel engaged in the sharing process are not all cleared to the same level of information. Thus, the complexity of secure information sharing is increased.

It is necessary to strike a balance between the critical need to provide an infrastructure that supports the real-time information sharing with the equally critical requirement to protect classified information from unauthorized access by someone not cleared for access to that information. Achieving this balance is not easy in any setting, whether in the real world or one that exists entirely within the CyberCIEGE game engine.

1. Specific Goals

The design of the AOC scenario had four specific educational goals. They are listed below. These include the four information assurance concepts that players are expected to learn in the game, and to get “right” in the real world after they have played the scenario and won.

   a. Networks that Exist at Different Levels of Classification Need to be Kept Separate

   Environments exist where networks, which contain information of different levels of classification must interact with each other. The only secure way to accomplish this interaction is with high assurance systems that can provide the appropriate protections for these multilevel connections. In the case of the AOC, the need for these interactions is minimal. The addition of expensive high assurance multilevel systems would add relatively little efficiency to the operation of the AOC. Therefore, it is in the best interests of the AOC environment to have the networks be exclusive to one level of classification to maximize security and keep costs low.
b. The Information at the Highest Level of Classification Needs to be Given the Most Consideration in Terms of Security.

It is necessary to protect information in a manner consistent with its sensitivity and value to the organization. In a hierarchical confidentiality system, the confidentiality labels indicate the relation of classification levels of assets to each other. Organizations with finite resources must allocate those resources to protect assets in accordance with its value as indicated by the confidentiality label. Resources include the funds spent on purchasing authentication mechanisms, initiating background checks for individuals in contact with the asset, or implementing physical security measures.

c. User Training, Physical Security, and Network Security Need to be Applied Together because Application of One is Ineffective without the Other

It is not possible to achieve effective protection of information on networked computers without evaluating the threat of attackers from every possible venue. Motivated attackers will attempt to gain access with a variety of approaches, e.g., Trojan horses, social engineering, and so forth. If the computers that store the information are locked in a vault, which requires multiple forms of authentication, but that machine is connected to a network, then the attacker has a way to work around the hardened physical security measures. In the same sense, if the computer is connected to an external network that has impenetrable safeguards in place, but physically resides in an unsecured area, then the information is again at risk. Adequate security cannot focus on one area for complete security, but rather must balance between user training, physical security, and network security.

d. Authentication Controls and Password Policies are a Suitable Defense Mechanism for Some Environments Having Shared Physical Space

The AOC environment’s main feature is that various levels of classification and user privilege share the same physical space. The security effectiveness of commercial authentication mechanisms depends on the physical circumstances. One possible situation involves shared space and limited physical controls so that users can see and touch machines for which they are not authorized. Another situation occurs when the attacker motive is very high, and subversion of the platform itself is a threat, undermining the commercial authentication mechanisms.
Without an objective basis for assuming that platforms have not been subverted, shared space is risky. Here the use of controlled space is advisable. A final situation exists when the motive is moderate and platform subversion is less likely. In this case, commercial-quality authentication mechanisms may be sufficient to mitigate the risk. Thus, strong password policies and authentication safeguards are a reasonable line of defense for protecting information on components.

2. The Scenario Gaming Approach

The AOC scenario is designed to teach these specific lessons through experience. The player is expected to repeatedly play the game, until the player wins the scenario.

One of the ways that the scenario promotes these lessons is by not making high assurance multilevel components available in the component catalog for the user to buy, which necessitates either a weak multilevel connection with a low assurance component or an exclusively single level design. The highest classified asset in the scenario causes the game to end if it is violated, forcing the problem of prioritizing security concerns to the forefront of the players’ considerations.

C. SCENARIO DEVELOPMENT APPROACH

The aforementioned educational goals led to the incremental development of the AOC scenario. The security topics determine all the choices in the scenario structure, which are impressed upon the player as encountered during the game.

Two playable zones comprise the AOC, which allows for the contrast between differing levels of physical security. The player can see the effects of compartmentalizing access for users. However, three levels of classification still exist, and only two zones are available for physical placement of users and components with assets. This drives the need for three different networks to be available in the General Access zone. Section E describes this situation in more detail.

Some assets in the AOC will be located on local machines that the user can access directly from the terminal. There are, however, other assets located at a physical location to which users do not have access. This aspect of the scenario truly drives the need for network connections to support achievement of asset goals by users.
Another important aspect of the scenario is the designer’s choice to collocate users with varying levels of secrecy clearance. In general, background checks are less thorough for users with low secrecy clearances. This choice punctuates the importance of strong authentication mechanisms on components in the General Access zone. This is because users with lower background checks, are more likely to perform insider attacks on components having high value assets to which they already have physical access. The only correct choice for the player is to ensure that only the users authorized to access components are able to access them. This is accomplished through the selection of strong authentication controls on the components.

D. SCENARIO BRIEFING

Players of the AOC scenario will read the following briefing as an introduction to their role in the game and the objectives they must achieve to win. This sample of the briefing displays diagrams that support the written paragraph, but these diagrams are restricted to this document, as the game briefing screen cannot display them. They could, however, be included in a text document copy of the briefing that may be distributed with the scenario upon its release. In terms of the descriptions of the scenario, users are the simulated workers in the game and players are the real people who play the game. In essence, the player serves the needs of the users in the CyberCIEGE world.

1. The Briefing

You are the Computer Networks Infrastructure (CNI) Officer for the communications element of the Air Operations Center (AOC), which controls all American military flights outside the United States to the Southern Hemisphere in support of the war on drugs in South America. The AOC is gearing up for an important series of events, during which operations will be very closely monitored and it is extremely important that all missions proceed without delay. The mission is to fight the aggressive actions of a very powerful drug-lord who has purchased surplus weapons and combat aircraft from the former Soviet Union military stockpile and is using these resources against his native government, an ally of the United States. The operations coordination by the AOC will include reconnaissance, search-and-rescue, direct air combat, and direct precision bombings of confirmed targets on the ground. To
accomplish these missions, the AOC is divided into cells, as shown in Figure 1, with each cell responsible for a specific aspect of operations support. These cells are divided between two divisions, the Plans Division and the Current Operations Division.

![AOC Conceptual Division of Labor](image)

Figure 1. AOC Conceptual Division of Labor

- **Plans Division**

  The Plans Division of the AOC is broken up into three cells: Intelligence Plans, Logistics Plans, and Weather Plans. Each cell has an external source of information that at least one of its members needs to access. In addition to this access, each cell also produces a document incorporated into the Air Tasking Order (ATO) by the ATO Production cell.

- **Intelligence Planning Cell**

  The Intelligence Plans Cell gathers all the inputs from government agencies (the United States and South American countries), news reports, previous battle information, military unit information, and human intelligence reports. Then, this cell processes all those items to produce a list of prioritized targets that will help to cripple the operations of the drug lord as well as minimize his ability to hurt innocent people in his country and manufacture and export illegal drugs out of the country. This list, called the Intel Target List, is submitted to the ATO production cell.

- **Logistics Planning Cell**

  The Logistics Plans Cell analyzes all the resources currently available to the military task force controlled by the AOC, such as all flight-worthy aircraft, fuel,
armaments, ammunition, funds, and available pilots and support personnel. Consequently, they produce a list of available aircraft for missions during the cycle, submitted to the ATO production cell, called the Logistics Resources List.

d. **Weather Planning Cell**

The Weather Planning Cell processes all long-range weather forecasts and compiles them into a list of areas in which the task force can operate missions during the ATO cycle. This list, called the Area Available List, is submitted to the ATO production cell.

e. **ATO Production Cell**

The ATO Production cell is the hardest working element of the AOC because it combines the products of all the Plans Division cells into the ATO, the critical flight plan document that allows the AOC to achieve its objectives. ATOs are produced every day for the following 24-hour period of missions. Figure 2 illustrates the products each cell submits to ATO production.

![Figure 2. Workflow in the Plans Division](image)

f. **Current Operations Division**

Once the ATO period of operations has begun, the plan is in effect, but plans never survive the first shot of the day. It is also necessary to make short-range adjustments to the ATO to ensure that missions are completed and objectives met during the 24-hour period of the ATO. The Current Operations Division contributes those
adjustments to “Plan B”, the altered ATO. Figure 3 outlines the flow of information in
the Current Ops Division based on the ATO, and indicates the specific right each cell
needs for each asset.

![Workflow in Current Ops Division](image)

**Figure 3. Workflow in Current Ops Division**

**g. Your Job**

Your goal in this scenario is to build and maintain the network
infrastructure, employ and train personnel, and buy and maintain the equipment to ensure
that it is possible to complete the mission. Each cell has a target goal of asset usage that
it must be able to maintain within the proper levels of secrecy to achieve success. If a
lack of availability or disclosure of the cell’s assets makes it impossible to achieve these
goals, monetary penalties will be assessed or for unavailability of high value assets the
game will end. Each asset in the scenario will have one of three different secrecy
classifications: TOP SECRET, SECRET, or UNCLASSIFIED. Each classification will
carry with it a value that represents its importance to the AOC in terms of dollars.

- **TOP SECRET** – Any asset or information classified as Top Secret is vital
to national security and serves as crucial information needed for military
operations. If this information is compromised, AOC operations will
cease. Additionally, any American citizen found trying to compromise
information at this level will be considered a traitor to the country and
executed.
• SECRET – Any asset or information that has been classified Secret is important to the operations of military forces. However, its value rests on its time-sensitive nature, and therefore, any violations will only have a temporary operational impact. The AOC will incur significant financial penalties due to time lost, but operations will continue. Anyone found mishandling or intentionally compromising Secret information will be stripped of all security clearances and detained. If the violators are civilian, they will be imprisoned for no less than two years and assessed a $10,000 fine.

• UNCLASSIFIED – Any information or asset that is unclassified is available to anyone in the military for official use. If civilians gain access to this information, it does not cause any significant harm to operations.

The secrecy classifications listed above are of a hierarchical nature, as shown in Figure 4. Therefore, a user who is cleared at the TOP SECRET level automatically has access to all information at the TOP SECRET, but can also read and write at the SECRET and UNCLASSIFIED levels.

![Hierarchy of Secrecy Classifications](image)

Figure 4. Hierarchy of Secrecy Classifications

Your sole objective is to avoid running out of money and to avoid disclosures of critical assets needed to keep the AOC communication network operational for 30 days. Moreover, if critical assets remain unavailable to users over an extended
period or become corrupted, the AOC mission will fail. If the AOC mission fails, the drug lords will dominate South America and numerous American lives will be lost in a long war of attrition.

E. SCENARIO DETAILS

This section describes the various parts of the SDF as they pertain to the scenario. The descriptions are not meant to be a narrative as much as they are meant to be a reference for readers regarding the specific values present in the SDF with an explanation of the value chosen, when needed. Also, the SDF syntax and layout are not ideal for easy reading and reference. Therefore, this section provides a clearer picture of the scenario itself. Not all variables in a section appear in this section, but rather a short explanation of the main driving variables appears. Specific variable names are highlighted for easy cross-reference to the SDF in the Appendix.

1. Organization

StartMoney represents the funds that players will have when starting the game. Given this pool of money, the player will have to make decisions about purchasing equipment, training personnel and hiring security and IT staff. To provide a challenge, the amount of $50,000 given to players will not provide the option of buying all possible secure components and hiring the best people in this scenario. The player must to balance between buying the best components, physical security, or background checks and user training.

Budget and ProfitShare dictate how fast the player’s available money will increase with the completion of certain goals of the scenario. The amount of cash in the AOC is the main indicator of success in the game. In the same manner, sudden losses of money are indicators of security breaches. In this scenario, the budget has been set at $10,000 and the profit share at 75%. This equates to a substantial rate of cash flow to the organization, which is sufficient to pay for guards, IT Support and to compensate for the cost incurred by successful attacks on SECRET assets, so that players may recover from one or two attacks without losing all money and ending the game.
2. Site

In this scenario, the “AOC Floor” is the only site supported. In future scenarios, however, it will be possible to represent organizations possessing multiple sites.

3. Zone

The Zone represents the main partition tool for the scenario designer when describing the envisioned general settings for a particular work area in the site. Each zone has a name and a site with which it is associated. This scenario will consist of three zones:

- General Access – The zone that encompasses the whole AOC.
- Reinforced Room – This is the zone intended for use by the player to secure most highly classified work. He is given the reinforced walls option at the start of the game, but everything else is the same as the General Access zone.
- Server Farm – This is a static zone, over which the player has no control. It is highly secured at the start of the game to house the servers that contain the majority of the assets that users of the scenario needs to gain access to via network connections.

All three zones have many physical security settings and procedural settings associated with them. The application of various physical security mechanisms will increase the physical security index of a zone, making it resistant to external attackers. For example, if an asset that has a attacker motive of 400 is located in a zone that has a physical security index of 500, then the asset is safe from external attackers walking up to that component and performing local attacks. This setting, however, has no bearing on network connections that may cross zones. A network connection is only as secure as the weakest zone to which it is connected.

4. Secrecy

The secrecy section defines the various SecrecyLabels that will play a role in the scenario. Three labels used in this scenario are Top Secret, Secret, and Unclassified, as previously discussed. The SecrecyValue and AttackerValue are the main driving forces of this variable’s importance in the scenario. The SecrecyValue is a monetary amount
designed to show the player how important assets of that classification are in terms of the classification hierarchy (i.e., Top Secret is the highest classification and also the most valuable).

The **AttackerValue** represents how badly an adversary wants to gain access to assets with those labels. This value is an integer value between 0 and 999. A setting of 600 on the Top Secret label appropriately indicates the extreme measures that attackers will employ to breach the security of assets with that label. These measures will indicate the skills of the professional attacker, versus amateur curiosity, and therefore, make the protection of Top Secret assets a challenge for the player.

The Secret label is given a setting of 400 to represent a greater-than-average interest by attackers to compromise assets of that classification. The player will be able to defend successfully against these attacks even when attackers have physical access to components containing these assets.

Assets labeled as Unclassified are set to 45, which represents a very low amateur interest in those assets.

5. **DAC Groups**

DAC Groups are the group designations used by the player to employ his discretionary access controls in the scenario. In the scenario as a simplification, these designations are predefined and are not modifiable by the player. A Public Group exists that includes all users. Additionally, a DAC Group exists for every cell in the scenario and alleviates the need to assign rights individually to an asset or to give access to a zone. DAC groups do not play a prominent role in this scenario, so the inclusion of DAC groups is more for the player to become familiar with seeing such group designations.

6. **Assets**

Assets are the main components of any CyberCIEGE scenario, creating the foundations upon which the rest of the game is played out. The important asset attributes to set are the **Secrecy** and the **CostList**. Attaching a Secrecy label to an asset also attaches an attacker motive to that asset, consequently dictating how much care the player has to take in securing it. In addition to the general attacker motive associated with the Secrecy label, the scenario designer can give a CostList value to the asset, which is a
penalty given for a specific violation of one or more rights, such as “read”, “write”, “modification”, or “execution”. It is also possible to shape this CostList specifically enough to focus on attacks perpetrated by an individual user or another DAC Group in the game. The CostList variable allows the flexibility to install insider attack weaknesses into the scenario in addition to general attacker motives. Only one CostList is used in the AOC scenario. It specifically focuses on the threat of insider attack from one member of the Weather Plans cell, as opposed to letting the game engine dictate those attacks. It gives the player someone to focus on when attempting to protect against insider attacks.

7. Asset Goals

Asset goals are the driving force behind user productivity and happiness in the game. These goals have nothing to do with security choices, by the player but they have everything to do with satisfying the virtual users. A general asset goal is defined and can then be assigned to one or more users. Included in the asset goal are the Asset to which it is attached and the Access Mode, which represents the rights that a user must have to the asset to fulfill his goal. If the Shared variable is set to “true”, all the users with this goal must be able to fulfill it or none of them will achieve the goal. Another degree of granularity that the scenario designer has available is to attach a specific piece of software or software type to the goal. In other words, it is not possible to achieve the goal unless that software is loaded on the component used to access the asset.

8. Users

Users have many different possible variables associated with them to shape the game experience for the player. Asset Goals are the most influencing setting in the user section as they describe what assets users must gain access to in order to be productive. A user may only have one asset goal or many different goals. Other important variables are user Trustworthiness and Initial Training. Trustworthiness is an indicator of how likely a user is to initiate an insider attack; low trustworthiness (below 50) is a high risk for malicious activity. While it is not possible to change the trustworthiness value during the game, it is possible, however, to augment it with Background Checks. The higher the background checks, the less likely the user will be to perform malicious actions against the enterprise. Initial Training represents the state of proficiency that the user has in terms of computer security training. This variable is an index from 0 to 100, where
the higher values affect how likely users are to follow the procedural security settings of components and zones. Lower values will increase the likelihood of security violations because users are not following the security protocols. It is possible to improve user training in the game, but that improvement comes at a cost. Training is available in low, medium, or high settings. Low training boosts the training of every user in the scenario by 1, medium by 5, and high by 10. For large enterprises with many users, this means that high training may not be possible due to costs associated with the training.

9. Components

The player begins this scenario with only four Targo Servers, which are located at the Server Farm location. It is necessary for the player to make network connections to these servers. Since the Server Farm is a static zone, the player can make no changes to its procedural or physical security. The only action needed is to connect the servers in that location to devices and purchased components for the users of the scenario. For the components purchased, it is necessary to make adjustments to the default procedural security settings in order for the components to be incorporated securely into the AOC infrastructure. The main areas to configure are the Network connections and the component procedural settings. Included in those settings are Boolean options such as LockorLogoff or WriteDownPassword, which affect to the overall security posture of the component.

10. Conditions and Triggers

Conditions and triggers are the elements of the SDF that allow the scenario designer to inject events into the game. There are several classes of conditions, listed in more detail in the Scenario Format Template (SFT) [Rivermind 2003]. They include:

- Average Cash
- Max Cash on Hand
- Minimum Cash on Hand
- Average User Happiness
- Average User Productivity
- Time Conditions
- User Happiness
- User Productivity
To set off triggers, it is possible to use these conditions individually or to connect them through Boolean operators. Triggers, as defined in the SFT [Rivermind 2003], are events that occur in the game but are not part of the normal game engine, defined by the scenario designer. They include:

- Win triggers
- Lose triggers
- Message triggers
- Ticker triggers
- Attack triggers
- Log triggers
- Budget triggers
- Happiness Adjustment trigger
- Productivity Adjustment trigger
- Change of Asset Target usage trigger
- Quit Game triggers
- Change Encyclopedia triggers
- Mask Attack trigger

This scenario contains only one Win trigger. However, there are several Lose triggers, illustrating the many ways to make mistakes and lose the scenario. Ticker, Message, and Budget triggers are also used in the scenario, but they are used more to simulate an AOC environment and less in support of the educational goal of the scenario.

F. GAME DESCRIPTIONS

The player of the game does not have access to the SDF, so all the information needed to succeed in the game will have to come from the descriptions provided in the various screens and informational sections of the game. Precise, unambiguous descriptions are critical for the player to have the best chance of achieving the game and learning objectives. There is, however, a need to make the descriptions entertaining and
to align them with the scenario premise. Below are the descriptions for the Users, Assets, and Asset Goals used in the game.

1. Users
   a. Maj Afinidad

   Maj Afinidad is an intelligence officer holding the position Chief of Intel Plans. She has very few skills aside from her position in Intelligence plans, but she is extremely loyal and trustworthy. She is the highest-ranking officer in the AOC, and therefore, the highest paid member. Her only asset goal is to read the Intel Feed.

   b. TSgt Miller

   TSgt Miller is an enlisted man in Intel Plans who has proven numerous times that he is trustworthy and a valuable resource to the AOC. He receives inputs from Maj Afinidad, and his primary asset goal is to create the Target List.

   c. TSgt Johnson

   TSgt Johnson, a Logistics Planner, is a consummate overachiever who does all the work in Logistics plans. He is 100% dedicated to his work in the AOC and highly trustworthy. He has two asset goals: to read the Logistics Resources Feed and to write the Logistics Resource List.

   d. TSgt Lewis

   TSgt Lewis is a Weather Analyst with a checkered past, which is why he is only granted access to unclassified information in Weather Plans. The only goal in his job is to access the Weather Feed.

   e. Capt Lisko

   Capt Lisko is 1999's Weather Officer of the Year and the current Weather Plans Cell Chief, selected because of his high degree of skill and ability to multitask. He has two asset goals: to read the weather feed and to write the Area Available List.

   f. Lt LaMore

   Lt LaMore is the ATO Production Chief, which is unheard of for a person of such low rank. However, she has proven through hard work and dedication that she is the most able person in the AOC, for which she was given the task of organizing inputs from four different assets and creating the ATO. She is definitely the most prepared officer in the AOC.
g. **TSgt Samuels**

TSgt Samuels is the Current Operations Division operator who dreams of someday joining the ranks of the officer corps. He is highly motivated to succeed in order to impress superiors into granting his wish. He does well splitting his efforts between reading the ATO and modifying Plan B.

2. **Assets**

a. **Intel Feed**

Intelligent software agents produce this feed. They employ web crawlers to search various intelligence sources for information on the region of interest. Intelligence is the critical source of information used to create the Target List. This feed is the backbone of the AOC, and its classification is Top Secret.

b. **Target List**

The Target List is a prioritized listing of all enemy locations valuable enough for missions to strike during the operating time of the next ATO (next 24-hour period). This list is incorporated into the ATO for targeting assignments and is classified Secret.

c. **Logistics Resource Feed**

This feed contains all inputs from units in the field on functional aircraft, fuel available, armament available, and spare parts. These inputs are all current numbers, and are not projections. This feed is classified Secret.

d. **Logistics Resource List**

This spreadsheet lists all resources that will be available for the next 24-hour period of operations by location and aircraft. The list is prioritized by order of aircraft that have the most fuel and armament resources available down to those that are low in resources. The Logistics Resource List is classified Secret.

e. **Weather Feed**

The Weather Feed is single page summary broadcast of results from several parsing programs that search the Internet for weather information related to the region in which the AOC is operating. Sources of information include local weather agencies, satellite information, and the national weather server. This feed is Unclassified.
f. **Area Available List**

This two-part document includes an electronic map listing and text document containing coordinate zones of areas with suitable weather conditions for missions in the 24-hour period of the ATO. The AAL is classified Secret.

g. **Air Tasking Order**

The ATO, the single most important document in the AOC, combines information from the Target List, the LRL, and the AAL into a prioritized listing of targets, which support the strategic goals of the AOC, have favorable weather conditions, and are attainable with current resources. A new ATO is published every 24 hours with a new listing of prioritized targets from new inputs from the various Planning Cells. The Air Tasking Order is classified Secret.

h. **Plan B**

Plan B is a version of the ATO modified in real time by the Current Ops Cells during the 24-hour period for which the ATO is in effect. All operational units refer to this document for information on current mission requirements and available resources.

3. **Asset Goals**

a. **Access Intel Feed**

The goal is to review data from the Intel Feed web page using any web browser software. It is critical to the AOC that the person who has this asset goal be able to fulfill it so that they can process the data and provide inputs to other members of Intel Plans.

b. **Produce Target List**

Through verbal communication and coordination during planning meetings, inputs are taken from the person assigned to process information from the Intel Feed and those inputs are organized in a logical listing of enemy targets called the Target List.

c. **Access Logistics Feed**

The goal is to be able to review the information pertaining to logistical resources by connecting to the Logistics Resources Feed on the Logistics Server.
d. **Produce LRL**

User processed information obtained from operational experience and inputs from the network feeds write the Logistics Resource List.

e. **Access Weather Feed**

This is a shared goal where all those who have this goal must be able to review the information available in the Weather Feed through a connection to the Weather Server.

f. **Produce AAL**

The goal is to use the information available to the weather cell to write the Area Available List.

g. **Produce ATO**

The goal is to take inputs from all three planning cells and the assets that they produce and write the Air Tasking Order for review by all members of Current Ops Cells.

h. **Access AAL**

The goal is to access the AAL produced by the Weather Plans Cell.

i. **Access LRL**

The goal is to access the LRL produced by the Logistics Plans Cell.

j. **Access Target List**

The goal is to access the Target List produced by the Intel Plans Cell.

k. **Access ATO**

This is a shared goal for all those who have it, where all must be able to read the ATO by whatever means necessary.

l. **Modify Plan B**

This plan Reads inputs from the ATO, and is able to write and modify the Plan, which is an asset located on a server.

G. **SUMMARY**

This chapter has outlined the basic structure of the AOC scenario as well as the educational goals of the scenario. It is only possible to observe the true impact of a scenario, however, during extensive testing, which validates whether or not the scenario
works in accordance with the security policies upon which its design is based. The next chapter introduces the methodology used to test this scenario and the lessons learned from the testing process.
III. SCENARIO TESTING

A. INTRODUCTION

This chapter describes the testing methodology employed and the results of that testing process. In the testing discussion, there are references to two scenario definitions. The first is the solution scenario, which is a complete definition that can be loaded into the game engine and run without modification to successful conclusion. The second is the playable scenario version, which is for distribution to players who can make modifications and additions to the initial state in an attempt to achieve a successful conclusion.

The testing objective was to map the educational goals stated in earlier chapters to specific observations of events in game play. Scenario testing was conducted in three phases: mini-scenarios development, correct solution testing, and bad security choice testing.

The early mini-scenarios were developed to test specific aspects of the game engine and educate the scenario designer on the effective use of those mechanisms in a larger scenario. Those results were also used as inputs to the game developers regarding potential problems in game code. However, the main objective for developing the mini-scenarios was to explore conceptual notions regarding specific security items in the game, thereby educating and training the scenario developer on how to incorporate those items effectively in his overall scenario.

The second phase was the correct solution testing, which focused on what choices the player had to make in order to achieve success in the scenario. This phase was important in terms of scenario development, but in terms of relating the educational goals of this thesis, the “bad security choice” phase of testing provides better information.

Bad security choice testing, the final phase, is the testing most relevant to mapping results to educational goals. This testing consisted of taking a preexisting solution and creating different scenarios from it by modifying one aspect to reflect a poor
security choice. The attacker AI of the game engine exploits the bad choices in these scenarios, which clearly illustrate the importance of principles cited in the educational goals section.

B. MINI-SCENARIO TESTING - PHASE I

The objective of mini-scenario development was to choose a game mechanism and explore its implementation and effects through a series of small scenarios. It is important to note that the game engine was in development during the time that these scenarios were being created. Hence, all unsuccessful test scenarios were later resolved with subsequent releases of the game.

The AOC scenario focuses on fulfillment of asset goals over network connections. These connections could network components that contain information of three different possible Secrecy levels, TOP SECRET, SECRET, or UNCLASSIFIED. Phase I testing focused on users achieving asset goals with variations in secrecy settings, shared asset goal settings, and network connection settings. Tables 1-5 in Phase I Test section have four columns indicating the scenario name, the scenario setting, the aspect of the scenario or game engine tested, and the results. Two columns of special interest are the testing aspect and results column for each scenario. These columns provide the best feedback for any necessary tuning of the scenario.

1. Basic Set

These sequences of scenarios were created to explore the basic relationships that exist in the scenario definition file between these various elements, e.g., organizations, sites, users and components. Cases are numbered incrementally to reflect absorption or modification of previous case elements:

2. Secrecy Label Set

This set of scenarios was created to explore the impact of variations of secrecy labels where users must create uninstantiated assets and achieve asset goals. Table 2 shows the results.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baseline.sdf</td>
<td>Includes one user</td>
<td>Basic Req's of the SDF format</td>
<td>Scenario runs</td>
</tr>
<tr>
<td>BasicSet1.sdf</td>
<td>Adds an un instantiated Asset and Asset Goal section to existing user</td>
<td>The user should be unhappy because he has an asset he cannot access</td>
<td>User cannot achieve success</td>
</tr>
<tr>
<td>BasicSet2.sdf</td>
<td>Adds a component to which the user has access</td>
<td>Given appropriate conditions, users create the assets for which they have goals on components</td>
<td>With a change to the component allocated secrecy label to Secret, the User creates asset on component</td>
</tr>
<tr>
<td>BasicSet2a.sdf</td>
<td>Asset is instantiated on the component provided</td>
<td>Given a component with the asset and access to it, user should be happy</td>
<td>User achieves his asset goal</td>
</tr>
<tr>
<td>BasicSet3.sdf</td>
<td>Takes one user and one component with no clearance. An asset is instantiated on the component</td>
<td>The user should get access to the asset for which he has an asset goal</td>
<td>The user was able to achieve his asset goal</td>
</tr>
</tbody>
</table>

Table 1. Basic Set Results

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecrecyLabelSet1.sdf</td>
<td>Takes one user and one component and adds the secrecy label of “Secret” to the asset. The component allocated secrecy list is cleared up to Secret and the user has a clearance of “Secret” The user will also have max training to avoid free variables</td>
<td>User should maintain access to the asset</td>
<td>User does maintain access</td>
</tr>
<tr>
<td>SecrecyLabelSet2.sdf</td>
<td>Takes two users, two assets, and two components. One set will be labeled with “Secret” and one with “Unclassified”.</td>
<td>Users creating assets on machines available to them</td>
<td>Assets are created on the appropriate components and users achieve asset goals</td>
</tr>
<tr>
<td>SecrecyLabelSet3.sdf</td>
<td>Takes one user and makes a component with “no restrictions” no Min/Max secrecy labels</td>
<td>See if the user creates his asset on a machine that allows all</td>
<td>User creates asset on component</td>
</tr>
<tr>
<td>SecrecyLabelSet4.sdf</td>
<td>Takes one user and makes a component with the restriction that nothing higher than Unclass be put on it.</td>
<td>User training should be followed and asset should not be created on lower classified component</td>
<td>User ignores training and creates asset on component</td>
</tr>
<tr>
<td>SecrecyLabelSet5.sdf</td>
<td>Takes two users, two assets, and two components. One asset will be labeled with “Secret” and one with “Unclassified”. In this case the posindex of the two users is switched, Unclass user in front of the Secret Component and Secret user in front of Unclass Component</td>
<td>User should maintain access to their assets regardless of relative position</td>
<td>Users both maintain access to their assets</td>
</tr>
</tbody>
</table>

Table 2. Secrecy Label Set Results
3. Shared Access Set

This set of tests explored variations associated with the access lists of a component when two users have asset goals to the same asset located on that component. In later versions of the mini scenarios, an added shared goal objective was added to observe how one user’s asset goal success rate would be affected if the other user cannot achieve their asset goal. Table 3 shows the results of this set of tests.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SharedAccessSet1.sdf</td>
<td>Takes two users with asset goals for the same asset, but only one of them gets a computer to work on and is on its access list. The shared asset is set to false. The asset will be instantiated. Secrecy Labels are not part of this test case.</td>
<td>See if the shared goal aspect works</td>
<td>Success</td>
</tr>
<tr>
<td>SharedAccessSet2.sdf</td>
<td>Takes two users with asset goals for the same asset, but only one of them gets a computer to work on and is on its access list. The shared asset is set to true. The asset will be instantiated.</td>
<td>Both users should fail their goal when both do not get access to the asset</td>
<td>Only one user fails their goal. This is a failed test?</td>
</tr>
<tr>
<td>SharedAccessSet3.sdf</td>
<td>Takes two users with asset goals for the same asset, but only one of them is on the access list for the computer. The shared asset boolean is omitted. The asset is instantiated.</td>
<td>See if both users get access</td>
<td>Success</td>
</tr>
<tr>
<td>SharedAccessSet4.sdf</td>
<td>Takes two users with asset goals for the same asset and both of them are on the access list for the machine. The shared asset boolean is set to true. The asset is instantiated.</td>
<td>See if both users get access</td>
<td>Success</td>
</tr>
</tbody>
</table>

Table 3. Shared Access Set Results

4. Attack Trigger Loss Set

The trigger element represents a measure of control that the scenario designer has over the game after gameplay has begun. In the AOC scenario, there are a variety of triggers in use, but the initial testing, as shown in Table 4, was conducted with the AttackSuccess trigger specifically in mind because a successful attack on the game’s highest classified asset, the Intel Feed, is a game-ending event. These initial trigger trial scenarios determined all later trigger development.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>AttackLossTrigger.sdf</td>
<td>Takes one user with an asset goal and the attacker setting at max</td>
<td>See if the game ends when the attack is successful</td>
<td>The game ends when an attack happens</td>
</tr>
<tr>
<td>AttackLossTrigger2.sdf</td>
<td>Takes one user with an asset goal and the attacker motive setting at 0</td>
<td>The game should keep going because there is no motive to attack the asset by anyone</td>
<td>No attack occurs. Success.</td>
</tr>
</tbody>
</table>

Table 4. Attack Loss Trigger Set Results

5. **Network Connections Set**

The AOC scenario has six networks in it. Thus, asset goal success over network connections is a key element of success in the scenario. These scenarios, as listed in Table 5, tested the ability to reach assets remotely via network connections.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetworkConnections1.sdf</td>
<td>Takes one user with an asset goal on a machine that he is connected to through the network</td>
<td>See if the asset goal is fulfilled by remote access</td>
<td>The asset goal is fulfilled</td>
</tr>
<tr>
<td>NetworkConnections2.sdf</td>
<td>Takes one user with an asset goal on a remote machine to which the player needs to create the connections to achieve success</td>
<td>Connect two machines via a cable and see if the asset goal is fulfilled</td>
<td>Once the player creates the network connections, the asset goal is fulfilled</td>
</tr>
</tbody>
</table>

Table 5. Network Connections Set Results

The lessons learned from designing these small scenarios were a pivotal step towards a proper development of the main scenario.

C. **CORRECT SOLUTION TESTING - PHASE 2**

The creation and testing of the solution scenario entailed a three-step approach. Step 1 was to write an entire solution in SDF format. That solution reflected all the choices the designer would have made as a player to achieve success given the objectives of the scenario. In other words, while there may be more than one “correct” solution that other players would employ for success, the designer only created one for testing.
This SDF was built incrementally by starting from a baseline scenario and adding all types of one game element to each successive step. The purpose was to reduce logic crash debugging with the game engine and maximize fine-tuning efforts on the scenario.

Table 6 below shows the fifteen scenarios that were the stepping stones to the large AOC scenario:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>BigScenario1.sdf</td>
<td>Basic Layout of the AOC. 1 Zone, 10 desks, no users.</td>
<td>No Testing</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario2.sdf</td>
<td>BigScenario1.sdf with additions</td>
<td>No Testing</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario3.sdf</td>
<td>BigScenario2.sdf with additions</td>
<td>No Testing</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario4.sdf</td>
<td>BigScenario3.sdf with asset goals for a user</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario5.sdf</td>
<td>BigScenario4.sdf with components to fulfill asset goals</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario6.sdf</td>
<td>BigScenario5.sdf with networked components</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario7.sdf</td>
<td>BigScenario6.sdf with an additional user</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario8.sdf</td>
<td>Same as BigScenario7.sdf</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario9.sdf</td>
<td>BigScenario8.sdf with all asset goals</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario10.sdf</td>
<td>Add asset goals and components to the Ops Division</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario10a.sdf</td>
<td>Incorporate all shared goals (all Ops cells to the ATO and Lisko and Lewis to the WxFeed)</td>
<td>Asset goals</td>
<td>Yes</td>
</tr>
<tr>
<td>BigScenario11.sdf</td>
<td>Securing SCIF Zone (Physical Access)</td>
<td>Physical security affecting attacks</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario12.sdf</td>
<td>Securing AOC Zone (Physical Access)</td>
<td>Physical security affecting attacks</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario13.sdf</td>
<td>Add software asset requirements to asset goals</td>
<td>Asset goals</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario14.sdf</td>
<td>Fix discretionary controls on Assets</td>
<td>Asset discretionary controls are more precise, limiting access to only those cells that require access for asset goals.</td>
<td>N/A</td>
</tr>
<tr>
<td>BigScenario15.sdf</td>
<td>Loss conditions</td>
<td>Added in loss conditions and triggers.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 6. AOC Scenario Development Steps
Many of the mechanical issues of the scenario were fixed during the step scenario development cycle used on the scenarios above. Once the basic issues had been resolved, completion of the final solution scenario was relatively simple. *AOCPlayablesolution.sdf*, located in section A of the Appendix, is the first completed scenario written by the scenario designer. It is complete because once loaded, it can be unpaused and run without modification to a successful conclusion.

The second part of the solution set three-step process was to take AOCPlayablesolution.sdf from section B of the Appendix and remove all components with the exception of servers located at the Server Farm Site, reset user training and background checks, and clear all server remote access lists. AOCPlayables.sdf, is the version meant for play by others and attached in section C of the Appendix. It represents an initial game state designed to let the player make many different choices, most of which will initially lead to failure. Eventually, however, a successful approach to the security choices required should become clear to any player and the objective achieved.

The designer played this playable version and his choices in the game reflected the hard coded settings from the complete solution, AOCPlayablesolution.sdf. Allowing enough elapsed game time to verify the completion of the correct security posture, this game was then saved, which generated another SDF: *AOCPlayablesolutionGame.sdf*. This version of the scenario is a hard coded version of all game play choices made by the designer in the test.

Once SDF versions AOCPlayablesolution.sdf and AOCPlayablesolutionGame.sdf were available, it was possible to compare them to each in terms of game elements present in the SDFs. This comparison verified that successful game play in the playable scenario does generate a SDF similar to the hard coded version originally written by the scenario designer.

Note, however, that the solution presented in this section is not intended to be conclusive. There is a large pool of possible decisions by players of the game that may lead to the same result, but would represent a different overall security posture and therefore a dissimilar SDF. This particular solution is provided as the one solution the scenario designer had in mind during scenario development.
D. BAD SECURITY CHOICE - PHASE 3

Phase III of testing was concerned with the poor security choices that players could make while playing the game. These choices relate directly back to the educational goals mentioned in the previous chapter. The intent is to illustrate the consequences of ignoring the specific lessons of the scenario.

Table 7 shows an overview of the test cases used and a brief description of the results observed.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Premise</th>
<th>Testing Aspect</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>BadSecurity10.sdf</td>
<td>All asset goals fulfilled and physical security in place. Background checks and user training has been left unmodified</td>
<td>Users with no background checks have access to TOP SECRET materials</td>
<td>The user with no background check performs insider attacks on the TOP SECRET asset and the game is over</td>
</tr>
<tr>
<td>BadSecurity6.sdf</td>
<td>All asset goals fulfilled physical security in place. Background checks and user training modified to a secure state. The S network is connected to LAN 1.</td>
<td>Having separately classified networks connected to each other without adequate protection mechanisms.</td>
<td>Insider attacks are performed by various users of the AOC in an effort to compromise the TOP SECRET asset</td>
</tr>
<tr>
<td>BadSecurity7.sdf</td>
<td>All asset goals fulfilled. Background checks and user training modified to a secure state. Physical security in the General Access zone and Reinforced Room zone are relaxed to a point below the motives of the assets located within them</td>
<td>Focus on network security while ignoring physical security</td>
<td>Assets are compromised by external attackers</td>
</tr>
<tr>
<td>BadSecurity8.sdf</td>
<td>All asset goals fulfilled and physical security at max. Background checks and user training modified to a secure state. Link encryptors are removed from network connections to Server Farm site.</td>
<td>Focus on physical security, while downplaying offsite network security</td>
<td>Assets at offsite locations should be compromised by external attackers via wiretap but are not. (This is a situation left to be resolved by game developers)</td>
</tr>
<tr>
<td>BadSecurity9.sdf</td>
<td>All asset goals fulfilled and physical security at max. Two networks LAN 1 and U are connected to the same component.</td>
<td>Having separately classified networks connected to each other without adequate protection mechanisms</td>
<td>A user with low security settings now has access to high classification assets via a network connection which he exploits repeatedly</td>
</tr>
<tr>
<td>BadSecurity11.sdf</td>
<td>Physical security settings of the General Access Zone are adequate, but Reinforced Room zone is left unsecured This gives SECRET cleared users access to the TOP SECRET area</td>
<td>Appropriate security procedures for higher levels of classified information</td>
<td>SECRET cleared users disclose or corrupt the TOP SECRET assets in the Reinforced Room zone</td>
</tr>
</tbody>
</table>

Table 7. Bad Security Choice Scenario Results
The following sections focus briefly on each situation listed above and explore the possible lessons learned from the results of game simulation.

1. **Insider Attacks – BadSecurity10.sdf and BadSecurity11.sdf**

   It is a common belief that the most dangerous attacker in any computer-networked environment is the malicious insider. They have the inside knowledge of security processes in the network and physical settings that allow them to gain access to assets that are untouchable by outsiders. In BadSecurity10.sdf, Major Afinidad has no background check. The value of the asset to which she has access, the Intel feed, is sufficient to override her trustworthiness and motivate an insider attack. In this example, the insider activity is limited to only those users who have access to the Reinforced Room zone and a medium or high background check is a viable solution to the problem of malicious insider activity in this zone. However, with larger groups of users, it is not practical to conduct extensive background checks on everyone who may be in physical proximity to high value assets. This illustrates the balance necessary between physical security, background checks, and authentication mechanisms. This means restricting high value assets to a zone where it is possible to tighten physical security and only a small group of authorized users in that zone would receive medium or high background checks. Combine these actions with authentication mechanisms, and malicious insiders remain with few opportunities to gain unauthorized access to assets.

   In BadSecurity11.sdf, the physical security part of that balance is omitted from internal security between the two zones. General Access physical security is adequate while Reinforced Room is not. The result of that missing piece is that users with SECRET and UNCLASSIFIED clearances are motivated to gain access to TOP SECRET assets and have the means to do so because there is no physical restriction to prevent this. In this particular scenario, several different users who would normally not have access to the Intel Feed completed insider attacks successfully. This again presses the importance of having complete security solutions.

2. **Network Separation – BadSecurity6.sdf**

   In this scenario, there are assets of different levels of classification. However, any one component only stores one such asset at a time. The Secrecy label attached to the asset dictates access to those components and the assets on them, i.e., users cleared to the
UNCLASSIFIED level have access to the component that stores an UNCLASSIFIED asset. Some users require access to assets of differing levels of classification and this access could be implemented through network connections between these components. Those multilevel network connections would require adequate protection mechanisms, which the designer has not provided as an option. Therefore, the networks must be separate from each other when those components are accessible by users of lower classifications. Ignorance of this lesson is apparent in BadSecurity6.sdf and BadSecurity9.sdf, where network connections are combined in one form or another. In these cases, a network connection is made from a lower level component to a higher level component, which in essence, grants a venue to a user of the lower level of classification to a higher level asset. Even though an explicit permission list giving those low users access to the higher level assets does not exist, the motivation to disclose those assets is enough for them to pursue access. In both cases, various users perform insider attacks, disclosing the higher level assets by exploiting the network connections. Once those network connections are separated again, the attacks on assets cease to occur.


Another critical tenet of this thesis is that complete security cannot exist while focusing solely on one area of the organization. It is essential to complement network security with comparable physical security settings, which must in turn, be supported by user training and background checks on internal users. In this test case, all settings related to user background checks and component securities have been maximized. The physical security posture of the two accessible zones of the AOC has been reduced to a level lower than that of the attacker motive of the assets in those zones. This creates a situation that is tempting to an external attacker, and network security mechanisms do not help to prevent those attackers from gaining access to the high value assets. This result stems from the fact that the external attack now has local access to the components that store high level assets and the motivation is is high enough to for the application of professional hacker techniques. Without the physical security piece, overall effective security is lost in this scenario.
4. **Network Security – BadSecurity8.sdf**

In this scenario, four of the assets users need to gain access to in order to achieve success are all located on components, which physically reside at another location. To gain access to those assets, it is necessary to extend network connections beyond the local site. One issue with this connection is that wires do not have any independent security properties, since their security relies on the security of the physical area where they are located. Hence, when a connection is made between two locations where the area between the two locations cannot be secured, other measures must be used. In the case of the AOC scenario, where the level of classification warrants it, link encryption is used on external wire connections to protect against wire tap attacks. This test illustrates that when link encryption devices are not employed, external attackers will gain access to the assets at the offsite location without ever having to step foot on either premises.

At the time, this scenario was created, the expected wire tap attack was not observed in game play, even though the motive was sufficient to warrant it. This flaw in the game engine was brought to the attention of the game developers for resolution.

**E. SUMMARY**

Testing occurred in three phases. The initial phase was performed in conjunction with scenario development to test the various aspects of the game engine that would be effective in the proposed scenario. Phase II of testing focused on the correct solution as given by the scenario designer as both the *hard coded* and *played* version. Finally, Phase III of testing lent itself entirely to the exploration of consequences incurred from poor security choices that violate the educational goals at the heart of this thesis. The next chapter will focus on the thesis’s conclusion as well as future work suggestions.
IV. CONCLUSION AND FUTURE WORK

A. CONCLUSION

This thesis is intended to provide answers to the two research questions stated in Chapter I. These questions drove the initial thought process and direction of the scenario design. Every step along the design path referred back to those questions in order to maintain a clear link to the foundation of the thesis.

The first question asks whether a CyberCIEGE scenario can accurately simulate a complex security environment. The AOC scenario discussed in this thesis does indeed portray the real-world issues present in AOC environments across the military forces. Having the research focus on multilevel security issues reflects true concerns in modern military operations. The resolutions to those issues presented in this thesis mirror practices that have become standard procedure across all branches of the U.S. military.

The second question focused on whether it was possible to write a scenario that could test the CyberCIEGE game engine’s ability to reflect a multilevel secrecy environment. It is the author’s argument that the game engine does indeed reflect a realistic simulation of the AOC scenario environment. This was verified by the fact that when the author applied his solution to the playable scenario, it could be completed by applying real-world practices observed in a true AOC.

This scenario is only the first step in harnessing the true power of the CyberCIEGE game engine and its ability to educate computer users. Hopefully, lessons can be learned from the development of this scenario and channeled into future development projects for scenarios that reflect a wide range of modern security environments in the modern world.

B. FUTURE WORK

Suggestions for future work are broken into two categories (listed below): those relating to future improvements of the AOC scenario and those relating to future exploration with CyberCIEGE scenarios in general.
1. **AOC Scenario Improvements**

The development of the AOC scenario occurred in conjunction with the development of the game engine. Due to the lack of maturity of the game engine and the timing of the developments, it was necessary to exclude many ambitious aspects of the scenario. When the game engine development has matured, it will be possible to explore some of the omitted aspects.

   a. **More Users Add More Complexity**

   The existence of only eight users in the scenario falls far short of the hundreds of users that operate in real-world Air Operations Centers. Future scenarios could include upgrades of certain cells in the AOC, populating the environment with more users and a larger variety of asset goals, which the player must satisfy.

   b. **Create a Multisite Scenario**

   An AOC does not operate as its own eyes and ears, instead it receives inputs from dozens of other units at geographically distant locations. These other sites were abstracted by the inclusion of the Server Farm in this version of the scenario. It would greatly enhance the realism of the scenario to create multiple sites, each with its own distinct network setup.

   c. **Introduce Integrity Issues**

   The issues relating to integrity of information and labels associated with integrity were not included in this version of the scenario. However, those issues are definitely relevant, and worth exploring in future scenario renditions.

   d. **Use of Triggers for Time Management Issues**

   Due to a compressed time schedule, not as much time had been devoted to experimentation and tuning of the various triggers and condition sets available in the game. Dedicating time to explore the use of triggers would greatly enhance future work. Triggers could focus on the time-critical nature of information in the AOC and create different network settings at different times during game play, forcing the player to respond actively to the game.

2. **General Scenario Work**

   In general, future work on CyberCIEGE scenarios would do well to focus on the multiplayer aspect of the game. This work would create situations where players could
confront each other as defender and attacker or players could work cooperatively as IT managers of different sites, which must communicate. Multiplayer scenarios are the best possible implementation of the power of CyberCIEGE, forcing players to work together in large decision processes.
This appendix contains the complete scenario definition code of the three SDF’s discussed in Chapter III, section C.

A. AOCPLAYABLESOLUTION.SDF

// Game generated save game file
// Real Time: Sat Jun 05 19:16:41 2004
// Game Time: Jan 1 08:00 am

Organization:
   Name: AOC :end
   Title: Air Operations Center :end
   UseWorkOffsiteOffice: False :end
   Internet: False :end
   UseSmallOffice: True :end
   StartMoney: 30000 :end
   Budget: 10000 :end
   StartMonth: 1 :end
   StartDay: 1 :end
   StartHour: 8 :end
   StartMinute: 0 :end
   UseWorkOffsiteOffice: False :end
   WorkSpaceFile: WorkSpaceAOC.txt :end
   ProfitSharing: 75 :end
:end // Organization Block

Site:
   Name: Air Operations Center Site :end
   Description: Air Operations Center :end
:end // Site Block

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

Network:
Name: U :end
:end // Network Block

Network:
Name: S :end
:end // Network Block

Network:
Name: TS :end
:end // Network Block

Network:
Name: Offsite TS Wire :end
:end // Network Block

Network:
Name: Offsite S Wire :end
:end // Network Block

Network:
Name: Offsite U Wire :end
:end // Network Block

Zone:
Name: AOC :end
Site: Air Operations Center Site :end
Art: smalloffice.tga :end
Description: :end
// Start Default Component Settings
ProtectWithACL: true :end
LockorLogoff: true :end
PasswordLength: Medium :end
PasswordCharacterSet: Moderate :end
PasswordChangeFrequency: six :end
NoEmailAttachmentExecute: true :end
NoWebMail: true :end
ApplyPatches: true :end
UserBackup: true :end
UpdateAntivirus: Regular :end
MaxSecrecyLabel: Secret :end
MinSecrecyLabel: Unclassified :end
MaxIntegrityLabel: :end
MinIntegrityLabel: :end
// End Default Component Settings
// Start Zone Security Settings
Receptionist: true :end
PatrollingGuard: true :end
VisualPeopleInspection: true :end
KeyLockOnDoor: true :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
SurveillanceCameras: true :end
ModerateIrisScanner: true :end
Badges: true :end
PermitEscortedVisitors: true :end
PermittedUsers: *.WxPlans :end
PermittedUsers: *.LogPlans :end
PermittedUsers: *.ATO :end
PermittedUsers: *.CurrentOps :end
Secrecy: Unclassified :end
Secrecy: Secret :end
// End Zone Security Settings
ULC: 30 55 :end
LRC: 58 32 :end
:end // Zone Block

Zone:
Name: SCIF :end
Site: Air Operations Center Site :end
Art: smallupperzone.tga :end
Description: :end
// Start Default Component Settings
ProtectWithACL: true :end
LockorLogoff: true :end
PasswordLength: Long :end
PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoMediaLeaveZone: true :end
NoWebMail: true :end
ApplyPatches: true :end
LeaveMachinesOn: true :end
UpdateAntivirus: Regular :end
MaxSecrecyLabel: Top Secret :end
MinSecrecyLabel: Secret :end
MaxIntegrityLabel: :end
MinIntegrityLabel: :end
// End Default Component Settings
// Start Zone Security Settings
GuardAtDoor: true :end
PatrollingGuard: true :end
KeyLockOnDoor: true :end
CipherLockOnDoor: true :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
ExpensiveIrisScanner: true :end
Badges: true :end
PermittedUsers: *.IntelPlans :end
Secrecy: Top Secret :end
// End Zone Security Settings
ULC: 39 50 :end
LRC: 50 44 :end
:end // Zone Block

Zone:
  Name: Server Farm :end
  Site: Air Operations Center Site :end
  Art: offsitezone.tga :end
  Description: :end
Static: true :end

// Start Default Component Settings
ProtectWithACL: true :end
LockorLogoff: true :end
PasswordLength: Long :end
PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoMediaLeaveZone: true :end
NoWebMail: true :end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UpdateAntivirus: Regular :end
MaxSecrecyLabel: Top Secret :end
MinSecrecyLabel: Unclassified :end
MaxIntegrityLabel: :end
MinIntegrityLabel: :end
// End Default Component Settings
// Start Zone Security Settings
Receptionist: true :end
GuardAtDoor: true :end
PatrollingGuard: true :end
VisualPeopleInspection: true :end
KeyLockOnDoor: true :end
CipherLockOnDoor: true :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
ModeratePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
XRayPackages: true :end
ExpensiveIrisScanner: true :end
ModerateIrisScanner: true :end
Badges: true :end
PermitEscortedVisitors: true :end
Secrecy: Top Secret :end
// End Zone Security Settings
ULC: 94 25 :end
LRC: 103 14 :end
:end // Zone Block

Department:
   Name: Current Ops :end
:end

Secrecy:
   Name: Unclassified :end
   Level: 1 :end
   Category: 0 :end
   SecrecyValue: 1000 :end
   SecrecyValueChange: 0 :end
   AttackerValue: 100 :end
   AttackerValueChange: 0 :end
   InitialBackGroundCheck: Medium :end
:end // Label Block

Secrecy:
   Name: Secret :end
   Level: 2 :end
   Category: 0 :end
   SecrecyValue: 4000 :end
   SecrecyValueChange: 0 :end
   AttackerValue: 300 :end
   AttackerValueChange: 0 :end
   InitialBackGroundCheck: Medium :end
:end // Label Block

Secrecy:
   Name: Top Secret :end
   Level: 3 :end
   Category: 0 :end
   SecrecyValue: 10000 :end
   SecrecyValueChange: 0 :end
   AttackerValue: 600 :end
   AttackerValueChange: 0 :end
   InitialBackGroundCheck: High :end
DACGroups:
  Group: WxPlans :end
  InitialBackGroundCheck: Low :end
  Group: IntelPlans :end
  InitialBackGroundCheck: Medium :end
  Group: LogPlans :end
  InitialBackGroundCheck: Medium :end
  Group: ATO :end
  InitialBackGroundCheck: Medium :end
  Group: CurrentOps :end
  InitialBackGroundCheck: Medium :end
: end // DAC Groups

Asset:
  Name: Intel Feed :end
  Description: This feed is produced via intelligent software agents that employ web crawlers to search various intelligence sources for information on the region of interest. It is the critical source of information used to create the Target List. This feed is the backbone of the AOC. Its classification is Top Secret. :end
  IsInstantiated: True :end
  Secrecy: Top Secret :end
  DOSMotive: 300 :end
  AvailabilityPenalty: 0 :end
  AccessList:
    *.IntelPlans YNNN
  : end // AccessList
  CostList:
    Access: *.Public :end
    AccessMode: NYNN :end
    Cost: 1000 :end
    AttackerMotive: 10 :end
  :end // CostList
  // Start Asset attacked history
  AttackHistory: 0 -1 -1 :end
  AttackHistory: 1 -1 -1 :end
  AttackHistory: 2 -1 -1 :end
  AttackHistory: 3 -1 -1 :end
  AttackHistory: 4 -1 -1 :end
  AttackHistory: 5 -1 -1 :end
Asset:
  Name: Target List :end
  Description: The Target List shows all enemy locations in prioritized order that of strategic importance for the success of missions run by the AOC. The targets are prioritized based off of information that is received from the Intel Feed. Its classification is Secret. :end
  IsInstantiated: True :end
  Secrecy: Secret :end
  DOSMotive: 0 :end
  AvailabilityPenalty: 0 :end
  AccessList:
    *.IntelPlans YYNN
    *.ATO YNNN
  :end //Accesslist
  CostList:
    Access: *.LogPlans :end
    AccessMode: NYNN :end
    Cost: 1000 :end
    AttackerMotive: 100 :end
  :end //CostList
// Start Asset attacked history
  AttackHistory: 0 -1 -1 :end
  AttackHistory: 1 -1 -1 :end
  AttackHistory: 2 -1 -1 :end
  AttackHistory: 3 -1 -1 :end
  AttackHistory: 4 -1 -1 :end
  AttackHistory: 5 -1 -1 :end
  AttackHistory: 6 -1 -1 :end
// End Asset attacked history
  :end // Asset

Asset:
  Name: Logistics Resources Feed :end
  Description: This feed updates all logistics information in the operational area. This feed is classified Secret :end
  IsInstantiated: True :end
  Secrecy: Secret :end
  DOSMotive: 0 :end
Asset:
  Name: Logistics Resource List :end
  Description: This is a spreadsheet of resources that will be available for the next 24 hour period of operations. The LRL is compiled from data received over the Logistics Resources Feed. The LRL is classified Secret. :end
  IsInstantiated: True :end
  Secrecy: Secret :end
  DOSMotive: 0 :end
  AvailabilityPenalty: 0 :end
  AccessList:
    *.LogPlans YYNN
    *.ATO YNNN
  :end //Accesslist
  CostList:
    Access: *.Public :end
    AccessMode: YYNN :end
    Cost: 100 :end
    AttackerMotive: 10 :end
  :end //CostList
  // Start Asset attacked history
  AttackHistory: 0 -1 -1 :end
  AttackHistory: 1 -1 -1 :end
  AttackHistory: 2 -1 -1 :end
  AttackHistory: 3 -1 -1 :end
  AttackHistory: 4 -1 -1 :end
  AttackHistory: 5 -1 -1 :end
  AttackHistory: 6 -1 -1 :end
  // End Asset attacked history
  :end // Asset
Asset:
   Name: Weather Feed
   Description: This feed is a collection of military and civilian weather tracking resources. This feed is Unclassified.
   IsInstantiated: True
   Secrecy: Unclassified
   DOSMotive: 0
   AvailabilityPenalty: 0
   AccessList:
      *.WxPlans YNNN
   CostList:
      Access: *.Public
      AccessMode: YYNN
      Cost: 0
      AttackerMotive: 0

Asset:
Name: Area Available List

Description: This listing shows all targets that have suitable weather conditions for the 24 hour period of the ATO. The AAL is based off of information received from the Weather Feed. The AAL is classified Secret.

IsInstantiated: True

Secrecy: Secret

DOSMotive: 0

AvailabilityPenalty: 0

AccessList:
*.WxPlans YYYY
*.ATO YNNN

CostList:
Access: *.Public
AccessMode: YNNN
Cost: 0
AttackerMotive: 0

// Start Asset attacked history
AttackHistory: 0 -1 -1
AttackHistory: 1 -1 -1
AttackHistory: 2 -1 -1
AttackHistory: 3 -1 -1
AttackHistory: 4 -1 -1
AttackHistory: 5 -1 -1
AttackHistory: 6 -1 -1
// End Asset attacked history

// Asset

Name: Air Tasking Order

Description: This listing of all missions planned for a 24 hour period. It is based off of inputs from the Target List, the Logistics Resources List, and the Area Available List. The Air Tasking Order is classified Secret.

IsInstantiated: True

Secrecy: Secret

DOSMotive: 50

AvailabilityPenalty: 1000

AccessList:
*.ATO YYYY
*.CurrentOps YNNN

CostList:
Access: *.Public
AccessMode: YNNN
Cost: 0
AttackerMotive: 0

// Start Asset attacked history
AttackHistory: 0 -1 -1
AttackHistory: 1 -1 -1
AttackHistory: 2 -1 -1
AttackHistory: 3 -1 -1
AttackHistory: 4 -1 -1
AttackHistory: 5 -1 -1
AttackHistory: 6 -1 -1
// End Asset attacked history


CostList:
  Access: *.WxPlans :end
  AccessMode: NYNN :end
  Cost: 1000 :end
  AttackerMotive: 10 :end
:end //CostList
// Start Asset attacked history
AttackHistory: 0 -1 -1 :end
AttackHistory: 1 -1 -1 :end
AttackHistory: 2 -1 -1 :end
AttackHistory: 3 -1 -1 :end
AttackHistory: 4 -1 -1 :end
AttackHistory: 5 -1 -1 :end
AttackHistory: 6 -1 -1 :end
// End Asset attacked history
:end // Asset

Asset:
  Name: Plan B :end
  Description: This is the altered ATO for reading and modification during the 24 flight period :end
  IsInstantiated: True :end
  Secrecy: Secret :end
  DOSMotive: 0 :end
  AvailabilityPenalty: 0 :end
  AccessList:
    *.CurrentOps YYNN :end
:end //Accesslist
CostList:
  Access: *.Public :end
  AccessMode: YYNN :end
  Cost: 0 :end
  AttackerMotive: 0 :end
:end //CostList
// Start Asset attacked history
AttackHistory: 0 -1 -1 :end
AttackHistory: 1 -1 -1 :end
AttackHistory: 2 -1 -1 :end
AttackHistory: 3 -1 -1 :end
AttackHistory: 4 -1 -1 :end
AttackHistory: 5 -1 -1 :end
AttackHistory: 6 -1 -1 :end
AttackHistory: 6 -1 -1 :end
// End Asset attacked history
:end // Asset

AssetGoal:
  Name: Access Intel Feed :end
  Description: Pull down data from the Intel Feed web page using any web browser software. It is critical to the AOC that the person who has this asset goal be able to fulfill it. :end
  Asset:
    Name: Intel Feed :end
    AccessMode: YNNN :end
  :end
  AvailabilityCostPenalty: 1000 :end
  :end // Asset Goal

AssetGoal:
  Name: Produce Target List :end
  Description: Be able to write and organize the prioritized Target List. :end
  Asset:
    Name: Target List :end
    AccessMode: NYNN :end
  :end
  AvailabilityCostPenalty: 500 :end
  :end // Asset Goal

AssetGoal:
  Name: Access Logistics Feed :end
  Description: This goal is to access the Logistics Feed through the use of web browser software. :end
  Asset:
    Name: Logistics Resources Feed :end
    AccessMode: YNNN :end
  :end
  AvailabilityCostPenalty: 70 :end
  :end // Asset Goal

AssetGoal:
  Name: Produce LRL :end
  Description: Be able to produce the Logistics Resource List. :end
  Asset:
    Name: Logistics Resource List :end
AssetGoal:
  Name: Access Weather Feed :end
  Description: This goal is to reach out to the Weather Feed and pull down data through the use of web browser software. :end
  Asset:
    Name: Weather Feed :end
    AccessMode: YNNN :end
    :end
    AvailabilityCostPenalty: 70 :end
    :end // Asset Goal

AssetGoal:
  Name: Produce AAL :end
  Description: This goal is to produce the Area Available List with any available spreadsheet software. :end
  Asset:
    Name: Area Available List :end
    AccessMode: NYNN :end
    :end
    AvailabilityCostPenalty: 70 :end
    :end // Asset Goal

AssetGoal:
  Name: Produce ATO :end
  Description: The Air Tasking Order (ATO) is produced and stands as the most important document in the AOC. :end
  Asset:
    Name: Air Tasking Order :end
    AccessMode: NYNN :end
    :end
    AvailabilityCostPenalty: 70 :end
    :end // Asset Goal

AssetGoal:
  Name: Access AAL :end
  Description: Access the AAL produced by the Weather Plans Cell using spreadsheet software. :end
Asset:
   Name: Area Available List :end
   AccessMode: YNNN :end
:end
   AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
   Name: Access LRL :end
   Description: Access the LRL produced by the Logistics Plans Cell using resource management software. :end
   Asset:
      Name: Logistics Resource List :end
      AccessMode: YNNN :end
:end
      AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
   Name: Access Target List :end
   Description: Access the Target List submitted by the Intel Plans Cell with spreadsheet. :end
   Asset:
      Name: Target List :end
      AccessMode: YNNN :end
:end
      AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
   Name: Access ATO :end
   Description: Be able to read the ATO. :end
   Asset:
      Name: Air Tasking Order :end
      AccessMode: YYNN :end
:end
      AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
   Name: Modify Plan B :end
   Description: Be able to modify the ATO to suit the needs of the battlefield today :end
Asset:
  Name: Air Tasking Order
  AccessMode: YYNN
  AvailabilityCostPenalty: 70

// Asset Goal

User:
  Name: Maj Afinidad
  Dept: Intel Plans Cell
  SecrecyClearance: Top Secret
  DACGroups:
    Public
    IntelPlans

// AssetGoal:
  AssetGoalName: Access Intel Feed
    TargetUsage: 10
    Happiness: 50
    Productivity: 86

// Trustworthiness: 100
// InitialTraining: 100
// Happiness: 70
// Productivity: 70
// Skill: 100
// HISupportSkill: 0
// HWSupportSkill: 0
// SWSupportSkill: 0
// PosIndex: 8
// Cost: 2000
// Gender: female

  UserDescription: Maj Afinidad is the Chief of Intel Plans with very few skills aside from her position in Intelligence plans and she has an asset goal to read the Intel Feed.

// User

User:
  Name: TSgt Miller
  Dept: Intel Plans Cell
  SecrecyClearance: Top Secret
DACGroups:
    Public :end
    IntelPlans :end :end
AssetGoal:
    AssetGoalName: Produce Target List :end
    TargetUsage: 80 :end
    Happiness: 50 :end
    Productivity: 48 :end :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 1 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Tsgt Miller is an Intel Planner and he has an asset goal to write the Target List :end :end // User
User:
    Name: T Sgt Johnson :end
    Dept: Logistics Plans Cell :end
    SecrecyClearance: Secret :end
    DACGroups:
        Public :end
        LogPlans :end :end
AssetGoal:
    AssetGoalName: Access Logistics Feed :end
    TargetUsage: 10 :end
    Happiness: 50 :end
    Productivity: 67 :end :end
AssetGoal:
    AssetGoalName: Produce LRL :end
TargetUsage: 90 :end
Happiness: 50 :end
Productivity: 29 :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 2 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Tsgt Johnson is a Logistics Planner who does all the work in Logistics plans, he has two asset goals, one to read the Logistics Resources Feed and one to write Logistics Resource List :end
User:
Name: TSgt Lewis :end
Dept: Weather Plans Cell :end
SecrecyClearance: Unclassified :end
DACGroups:
   Public :end
   WxPlans :end
AssetGoal:
   AssetGoalName: Access Weather Feed :end
   TargetUsage: 100 :end
   Happiness: 100 :end
   Productivity: 95 :end
   Trustworthiness: 100 :end
   InitialTraining: 100 :end
   Happiness: 70 :end
   Productivity: 70 :end
   Skill: 100 :end
   HISupportSkill: 0 :end
   HWSupportSkill: 0 :end
   SWSupportSkill: 0 :end
User:  
   Name: Capt Lisko  
   Dept: Logistics Plans Cell  
   Secrecy Clearance: Secret  
   DAC Groups:  
      Public  
      Wx Plans  
   
AssetGoal:  
   AssetGoalName: Access Weather Feed  
   Target Usage: 20  
   Happiness: 50  
   Productivity: 10  
AssetGoal:  
   AssetGoalName: Produce AAL  
   Target Usage: 80  
   Happiness: 50  
   Productivity: 86  
Trustworthiness: 100  
Initial Training: 100  
Happiness: 70  
Productivity: 70  
Skill: 100  
HISupportSkill: 0  
HWSupportSkill: 0  
SWSupportSkill: 0  
Pos Index: 6  
Cost: 2000  
Gender: male  
UserDescription: Capt Lisko is the Weather Plans Cell Chief and he has to read the weather feed and write the Area Available List
User:
   Name: Lt LaMore
   Dept: ATO Production Cell
   Secrecy Clearance: Top Secret
   DAC Groups:
      Public
      ATO
   :end
AssetGoal:
   AssetGoal Name: Produce ATO
   Target Usage: 70
   Happiness: 40
   Productivity: 38
   :end
AssetGoal:
   AssetGoal Name: Access AAL
   Target Usage: 10
   Happiness: 20
   Productivity: 19
   :end
AssetGoal:
   AssetGoal Name: Access LRL
   Target Usage: 10
   Happiness: 20
   Productivity: 19
   :end
AssetGoal:
   AssetGoal Name: Access Target List
   Target Usage: 10
   Happiness: 20
   Productivity: 19
   :end
Trustworthiness: 100
Initial Training: 100
Happiness: 70
Productivity: 70
Skill: 100
HISupportSkill: 0
HWSupportSkill: 0
SWSupportSkill: 0
PosIndex: 3
Cost: 2000
Gender: female

UserDescription: Lt LaMore is the ATO Production Chief and hardest working member of the AOC, he has four Asset goals. He needs to read the AAL, LRL, and the Target List while also being able to write the Air Tasking Order.

User:
Name: TSgt Samuels
Dept: Current Operations
SecrecyClearance: Secret
DACGroups:
  Public
  CurrentOps
AssetGoal:
  AssetGoalName: Access ATO
  TargetUsage: 50
  Happiness: 50
  Productivity: 48
AssetGoal:
  AssetGoalName: Modify Plan B
  TargetUsage: 50
  Happiness: 50
  Productivity: 48
Trustworthiness: 100
InitialTraining: 100
Happiness: 70
Productivity: 70
Skill: 100
HISupportSkill: 0
HWSupportSkill: 0
SWSupportSkill: 0
PosIndex: 4
Cost: 2000
Gender: male :end
UserDescription: Tsgt Samuels is a Air Defense Operator :end :end // User

User:
Name: A1C Boxer :end
Dept: Security :end
Secrecy Clearance: Unclassified :end
DACGroups:
  Public :end :end
  Trustworthiness: 100 :end
  Initial Training: 100 :end
  Happiness: 70 :end
  Productivity: 70 :end
  Skill: 100 :end
  HISupportSkill: 0 :end
  HWSupportSkill: 0 :end
  SWSupportSkill: 0 :end
  PosIndex: 0 :end
  Cost: 2000 :end
  Gender: male :end
UserDescription: A1C Boxer is a security forces troop :end :end // User

User:
Name: A1C Klinger :end
Dept: Security :end
Secrecy Clearance: Unclassified :end
DACGroups:
  Public :end :end
  Trustworthiness: 100 :end
  Initial Training: 100 :end
  Happiness: 70 :end
  Productivity: 70 :end
  Skill: 100 :end
  HISupportSkill: 0 :end
  HWSupportSkill: 0 :end
  SWSupportSkill: 0 :end
User:
Name: Randy: end
Dept: Tech :end
SecrecyClearance: Unclassified :end
DACGroups:

Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 90 :end
HISupportSkill: 80 :end
HWSupportSkill: 80 :end
SWSupportSkill: 80 :end
PosIndex: 3 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Randy is an ex-hacker working for the government :end
:end // User

User:
Name: Randy, too :end
Dept: Tech :end
SecrecyClearance: Unclassified :end
DACGroups:

Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 99 :end
HISupportSkill: 80 :end
HWSupportSkill: 80
SWSupportSkill: 80
PosIndex: 5
Cost: 2000
Gender: male
UserDescription: Randy is an ex-farmer working for the government

User:
Name: Randy, as well
Dept: Tech
SecrecyClearance: Unclassified
DACGroups:
  Public

Trustworthiness: 100
InitialTraining: 100
Happiness: 70
Productivity: 70
Skill: 99
HISSupportSkill: 80
HWSupportSkill: 80
SWSupportSkill: 80
PosIndex: 6
Cost: 2000
Gender: male
UserDescription: Randy is an ex-stock broker working for the government

Component:
Name: Afinidad Machine
IsTemplate: false
AssetProtection: True
HW: Blato Desktop Select
Static: false
Availability: 99
Resale: 600
OS: Populos V9 Desktop
Software: WordSmyth
Software: Internet Contemplator
Software: Extortos :end
UseBiometrics: true :end
AutomaticLockLogout: true :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: Automatic :end
ConfigUpdateAntivirus: Automatic :end
CM: Weak :end
User: Maj Afinidad :end
PosIndex: 8 :end
AccessListLocal: Maj Afinidad :end
AccessListRemote: Maj Afinidad :end
Network:
   Name: TS :end
:end // of network description
ComponentProceduralSettings:
ProtectWithACL: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoMediaLeaveZone: true :end
LeaveMachinesOn: true :end
OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
   Name: Intel Server :end
IsTemplate: false :end
AssetProtection: True :end
HW: Targo Server :end
Static: false :end
Availability: 99 :end
Resale: 600 :end
OS: Populos V9 Server :end
Software: Internet Contemplator :end
Software: Extortos :end
UseBiometrics: true :end
ScanEmailAttachments: true :end

69
StripEmailAttachments: true :end
AutomaticLockLogout: true :end
SelfAdminister: true :end
AdministerSoftwareControl: true :end
BlockRemovableMedia: true :end
BlockLocalStorage: true :end
BrowserSettings: Strict :end
EmailSettings: Strict :end
UpdatePatches: Automatic :end
UpdateAntivirus: Regular :end
ConfigUpdateAntivirus: Automatic :end
CM: Weak :end
PosIndex: 9 :end
Assets: Intel Feed :end
AccessListRemote: Maj Afinidad :end
Network:
    Name: Offsite TS Wire :end
:end // of network description
ComponentProceduralSettings:
ProtectWithACL: true :end
LockorLogoff: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoMediaLeaveZone: true :end
NoWebMail: true :end
LeaveMachinesOn: true :end
OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component
Component:
    Name: Miller Machine :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 99 :end
Resale: 600 :end
OS: Populos V9 Desktop :end
Software: Internet Contemplator :end
Software: Extortos :end
AutomaticLockLogout: true :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: Automatic :end
ConfigUpdateAntivirus: Automatic :end
CM: Weak :end
User: TSgt Miller :end
PosIndex: 1 :end
Assets: Target List :end
AccessListLocal: TSgt Miller :end
AccessListRemote: TSgt Miller :end
AccessListRemote: Lt LaMore :end
Network:
   Name: S :end
   :end // of network description
ComponentProceduralSettings:
   ProtectWithACL: true :end
   PasswordLength: Long :end
   PasswordCharacterSet: Any :end
   PasswordChangeFrequency: two :end
   NoMediaLeaveZone: true :end
   LeaveMachinesOn: true :end
   OffsiteBackup: true :end
   :end // ComponentProceduralSettings
   :end // Component

Component:
   Name: Johnson Machine :end
   IsTemplate: false :end
   AssetProtection: True :end
   HW: Blato Desktop Select :end
   Static: false :end
   Availability: 99 :end
   Resale: 600 :end
OS: Populos V9 Desktop
Software: Internet Contemplator
Software: Extortos
ScanEmailAttachments: true
StripEmailAttachments: true
AutomaticLockLogout: true
SelfAdminister: true
AdministerSoftwareControl: true
BlockRemovableMedia: true
BlockLocalStorage: true
BrowserSettings: Strict
EmailSettings: Strict
UpdatePatches: Automatic
ConfigUpdateAntivirus: Automatic
CM: Weak
User: TSgt Johnson
PosIndex: 2
Assets: Logistics Resource List
AccessListLocal: TSgt Johnson
AccessListRemote: TSgt Johnson
AccessListRemote: Lt LaMore
Network:
    Name: S
ComponentProceduralSettings:
    ProtectWithACL: true
    PasswordLength: Long
    PasswordCharacterSet: Any
    PasswordChangeFrequency: two
    NoMediaLeaveZone: true
    LeaveMachinesOn: true
    OffsiteBackup: true
Component:
    Name: Logistics Server
    IsTemplate: false
    AssetProtection: True
HW: Targo Server :end
Static: false :end
Availability: 99 :end
Resale: 600 :end
OS: Populos V9 Server :end
Software: Internet Contemplator :end
Software: Extortos :end
AutomaticLockLogout: true :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
CM: Weak :end
PosIndex: 10 :end
Assets: Logistics Resources Feed :end
AccessListRemote: TSgt Johnson :end
Network:
  Name: Offsite S Wire :end
  :end // of network description
ComponentProceduralSettings:
ProtectWithACL: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoMediaLeaveZone: true :end
LeaveMachinesOn: true :end
OffsiteBackup: true :end
  :end // ComponentProceduralSettings
  :end // Component
Component:
  Name: Weather Server :end
IsTemplate: false :end
AssetProtection: True :end
HW: Targo Server :end
Static: false :end
Availability: 99 :end
Resale: 600 :end
OS: Populos V9 Server :end
Software: Internet Contemplator :end
Software: Viewpoint :end
AutomaticLockLogout: true :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
CM: Weak :end
PosIndex: 11 :end
Assets: Weather Feed :end
AccessListRemote: TSgt Lewis :end
AccessListRemote: Capt Lisko :end
Network:
  Name: Offsite U Wire :end
  AccessList: *.WxPlans :end AccessMode: YYNN :end
:end // of network description
ComponentProceduralSettings:
  ProtectWithACL: true :end
  PasswordLength: Long :end
  PasswordCharacterSet: Any :end
  PasswordChangeFrequency: two :end
  NoMediaLeaveZone: true :end
  LeaveMachinesOn: true :end
  OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
  Name: Lewis Machine :end
  IsTemplate: false :end
  AssetProtection: True :end
  HW: Blato Desktop Select :end
  Static: false :end
  Availability: 99 :end
  Resale: 600 :end
  OS: Populos V9 Desktop :end
  Software: Internet Contemplator :end
  Software: Extortos :end
  AutomaticLockLogout: true :end
  BrowserSettings: Loose :end
  EmailSettings: Loose :end
  CM: Weak :end
  User: TSgt Lewis :end
  PosIndex: 5 :end
AccessListLocal: TSgt Lewis :end
AccessListRemote: TSgt Lewis :end

Network:
    Name: U :end
    AccessList: *.WxPlans :end AccessMode: YYNN :end
:end // of network description
ComponentProceduralSettings:
    ProtectWithACL: true :end
    PasswordLength: Long :end
    PasswordCharacterSet: Any :end
    PasswordChangeFrequency: two :end
    NoMediaLeaveZone: true :end
    LeaveMachinesOn: true :end
    OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
    Name: Lisko Unclass Machine :end
    IsTemplate: false :end
    AssetProtection: True :end
    HW: Blato Desktop Select :end
    Static: false :end
    Availability: 99 :end
    Resale: 600 :end
    OS: Populos V9 Desktop :end
    Software: Internet Contemplator :end
    Software: Extortos :end
    AutomaticLockLogout: true :end
    BrowserSettings: Loose :end
    EmailSettings: Loose :end
    CM: Weak :end
    User: Capt Lisko :end
    PosIndex: 6 :end
    AccessListLocal: Capt Lisko :end
    AccessListRemote: Capt Lisko :end
    AccessListRemote: *.Public :end
Network:
    Name: U :end
    AccessList: *.WxPlans :end AccessMode: YYNN :end
ComponentProceduralSettings:
ProtectWithACL: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoMediaLeaveZone: true :end
LeaveMachinesOn: true :end
OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
Name: Lisko Secret Machine :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 99 :end
Resale: 600 :end
OS: Populos V9 Desktop :end
Software: Internet Contemplator :end
Software: Extortos :end
AutomaticLockLogout: true :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
CM: Weak :end
User: Capt Lisko :end
PosIndex: 7 :end
Assets: Area Available List :end
AccessListLocal: Capt Lisko :end
AccessListRemote: Lt LaMore :end
Network:
Name: S :end
AccessList: *.WxPlans :end AccessMode: YYNN :end
:end // of network description
ComponentProceduralSettings:
ProtectWithACL: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoMediaLeaveZone: true :end
LeaveMachinesOn: true :end
OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
  Name: LaMore Machine :end
  IsTemplate: false :end
  AssetProtection: True :end
  HW: Blato Desktop Select :end
  Static: false :end
  Availability: 99 :end
  Resale: 600 :end
  OS: Populos V9 Desktop :end
  Software: Internet Contemplator :end
  Software: Extortos :end
  AutomaticLockLogout: true :end
  BrowserSettings: Loose :end
  EmailSettings: Loose :end
  CM: Weak :end
  User: Lt LaMore :end
  PosIndex: 3 :end
  Assets: Air Tasking Order :end
  AccessListLocal: Lt LaMore :end
  AccessListRemote: Lt LaMore :end
  AccessListRemote: *.CurrentOps :end
Network:
  Name: S :end
  AccessList: *.ATO :end
  AccessMode: YYNN :end
:end // of network description
ComponentProceduralSettings:
  ProtectWithACL: true :end
  PasswordLength: Long :end
  PasswordCharacterSet: Any :end
  PasswordChangeFrequency: two :end
  NoMediaLeaveZone: true :end
  LeaveMachinesOn: true :end
  OffsiteBackup: true :end
Component:
  Name: Plan B Server :end
  IsTemplate: false :end
  AssetProtection: True :end
  HW: Targo Server :end
  Static: false :end
  Availability: 99 :end
  Resale: 600 :end
  OS: Populos V9 Server :end
  Software: Internet Contemplator :end
  Software: Extortos :end
  AutomaticLockLogout: true :end
  BrowserSettings: Loose :end
  EmailSettings: Loose :end
  UpdatePatches: Automatic :end
  ConfigUpdateAntivirus: Automatic :end
  CM: Weak :end
  PosIndex: 12 :end
  Assets: Plan B :end
  AccessListRemote: *.ATO :end
  AccessListRemote: *.CurrentOps :end
Network:
  Name: Offsite S Wire :end
: end // of network description
ComponentProceduralSettings:
  ProtectWithACL: true :end
  PasswordLength: Long :end
  PasswordCharacterSet: Any :end
  PasswordChangeFrequency: two :end
  NoMediaLeaveZone: true :end
  LeaveMachinesOn: true :end
  OffsiteBackup: true :end
: end // ComponentProceduralSettings
: end // Component

Component:
Name: Samuels Machine :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 99 :end
Resale: 600 :end
OS: Populos V9 Desktop :end
Software: Internet Contemplator :end
Software: Viewpoint :end
AutomaticLockLogout: true :end
BrowserSettings: Loose :end
EmailSettings: Loose :end
UpdatePatches: Automatic :end
ConfigUpdateAntivirus: Automatic :end
CM: Weak :end
User: TSgt Samuels :end
PosIndex: 4 :end
AccessListLocal: TSgt Samuels :end
AccessListRemote: TSgt Samuels :end
Network:
  Name: S :end
:end // of network description
ComponentProceduralSettings:
ProtectWithACL: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoMediaLeaveZone: true :end
LeaveMachinesOn: true :end
OffsiteBackup: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
  Name: TS Encryptor AOC :end
  IsTemplate: false :end
  Resale: 600 :end
  AssetProtection: True :end
HW: Enigma2000 :end
Static: false :end
PosIndex: 8 :end
Network:
    Name: TS :end :end // of network description
AttachDevice: TS Encryptor Offsite :end :end // Device

Component:
    Name: TS Encryptor Offsite :end
    IsTemplate: false :end
    Resale: 600 :end
    AssetProtection: True :end
HW: Enigma2000 :end
Static: false :end
PosIndex: 9 :end
Network:
    Name: Offsite TS Wire :end :end // of network description
AttachDevice: TS Encryptor AOC :end :end // Device

Component:
    Name: S Encryptor AOC :end
    IsTemplate: false :end
    Resale: 600 :end
    AssetProtection: True :end
HW: Enigma2000 :end
Static: false :end
PosIndex: 2 :end
Network:
    Name: S :end :end // of network description
AttachDevice: S Encryptor Offsite :end :end // Device

Component:
    Name: S Encryptor Offsite :end
    IsTemplate: false :end
Resale: 600 :end
AssetProtection: True :end
HW: Enigma2000 :end
Static: false :end
PosIndex: 10 :end
Network:
    Name: Offsite S Wire :end
:end // of network description
AttachDevice: S Encryptor AOC :end
:end // Device

Component:
    Name: U Encryptor AOC :end
    IsTemplate: false :end
    Resale: 600 :end
    AssetProtection: True :end
    HW: Enigma2000 :end
    Static: false :end
    PosIndex: 5 :end
    Network:
        Name: U :end
    :end // of network description
AttachDevice: U Encryptor Offsite :end
:end // Device

Component:
    Name: U Encryptor Offsite :end
    IsTemplate: false :end
    Resale: 600 :end
    AssetProtection: True :end
    HW: Enigma2000 :end
    Static: false :end
    PosIndex: 11 :end
    Network:
        Name: Offsite U Wire :end
    :end // of network description
AttachDevice: U Encryptor AOC :end
:end // Device

OPTIONS:
UseScenarioCatalogItems: No :end :end

Briefing:
You are the IT manager for the AOC. See the Game description tab for objectives.
(PARAGRAPH)
:end // Briefing

Conditions:

Condition:
Tagname: Bankrupt :end
Parameter: 0 :end
Parameter: 1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: MinCashOnHand :end :end

Condition:
Tagname: MillerLackofProduct :end
ConditionText: TSgt Miller :end
Parameter: 0 :end
Parameter: 40 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: UserProductivity :end :end

Condition:
Tagname: IntelPlansGoalFailure :end
ConditionText: Maj Afinidad :end
SecondConditionText: Access Intel Feed :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Condition:
   Tagname: LogPlansGoalFailure :end
   ConditionText: TSgt Johnson :end
   SecondConditionText: Access Logistics Feed :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   ConditionClass: UserFailsGoal :end
:end

Condition:
   Tagname: FiveDays :end
   Parameter: 120 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   ConditionClass: TimeCondition :end
:end

Condition:
   Tagname: ThreeDays :end
   Parameter: 72 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   ConditionClass: TimeCondition :end
:end
Condition:
   Tagname: TSHack :end
   ConditionText: Intel Feed :end
   Parameter: 2 :end
   Parameter: 600 :end
   Parameter: 900 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   ConditionClass: AssetAttacked :end
: end

Condition:
   Tagname: TSHackInternal :end
   ConditionText: Intel Feed :end
   Parameter: 1 :end
   Parameter: 600 :end
   Parameter: 900 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   ConditionClass: AssetAttacked :end
: end

Condition:
   Tagname: MostestMoney :end
   Parameter: 10000 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   Parameter: -1 :end
   ConditionClass: MaxCashOnHand :end
: end

Condition:
   Tagname: MonthLong :end
   Parameter: 720 :end
   Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
  ConditionClass: TimeCondition :end
: end

Condition:
  Tagname: OneDay :end
  Parameter: 24 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  ConditionClass: TimeCondition :end
  : end

: end // Of Conditions

Triggers:
  Trigger:
    TriggerName: GameLostCash :end
    TriggerText: You are not that well funded
      (PARAGRAPh)
      : end
    FixedDelay: 0.000000 :end
    RandomDelay: 0.000000 :end
    FrequencyInDays: 0.500000 :end
    ConditionList: Bankrupt :end
    TriggerClass: LoseTrigger :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
  : end

Trigger:
  TriggerName: GameLostProduce :end
TriggerText: Intel Plans was not able to produce the Target List for at least a day, this is detrimental to the mission of the AOC:

FixedDelay: 1.000000
RandomDelay: 1.000000
FrequencyInDays: 0.500000
ConditionList: MillerLackofProduct
TriggerClass: LoseTrigger
Parameter: -1
Parameter: -1
Parameter: -1
Parameter: -1
Parameter: -1
Parameter: -1

Trigger:
TriggerName: BudgetReallocation
TriggerText: A portion of your budget has been reallocated to support the fight against Canada:
FixedDelay: 0.000000
RandomDelay: 15.000000
FrequencyInDays: 0.400000
ConditionList: ThreeDays
TriggerClass: BudgetTrigger
Parameter: -8000
Parameter: -1
Parameter: -1
Parameter: -1
Parameter: -1
Parameter: -1

Trigger:
TriggerName: FailedIntelGoal
TriggerText: Maj Afinidad is not able to fulfill her asset goal, make sure she has the means to her goal:
FixedDelay: 0.000000
RandomDelay: 0.000000
FrequencyInDays: 0.500000
ConditionList: IntelPlansGoalFailure
TriggerClass: MessageTrigger
Parameter: -1
Trigger:
  TriggerName: FailedLogGoal :end
  TriggerText: TSgt Johnson is not able to fulfill his asset goal to read the logistics feed, make sure he has the means to his goal :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.900000 :end
  ConditionList: LogPlansGoalFailure :end
  TriggerClass: MessageTrigger :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
:end

Trigger:
  TriggerName: LoseByAttackSuccess :end
  TriggerText: The Intel Feed was compromised by an external attacker, you are an idiot. :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: TSHack :end
  TriggerClass: LoseTrigger :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
:end
Trigger:

  TriggerName: LosebyAttackSuccess2 :end
  TriggerText: The Intel Feed was compromised by an internal attacker, you are betrayed. :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: TSHackInternal :end
  TriggerClass: LoseTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end

:end

Trigger:

  TriggerName: WinCashOverTime :end
  TriggerText: You have operated for 30 days, you have achieved victory :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: MonthLong :end
  TriggerClass: WinTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end

:end

Trigger:

  TriggerName: ATOPublished :end
  TriggerText: The ATO has been published :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: OneDay :end
  TriggerClass: TickerTrigger :end
B. AOCPLAYABLE.SDF

// Air Operations Center
// ATO Productions Playable Scenario

Organization:

Name: AOC :end
Title: Air Operations Center :end
StartMoney: 50000 :end
Budget: 10000 :end
StartMonth: 1 :end
StartDay: 1 :end
StartHour: 8 :end
StartMinute: 00 :end
UseSmallOffice: true :end
WorkSpaceFile: WorkSpaceAOC.txt :end
ProfitSharing: 75 :end
Internet: false :end

Site:

Name: Air Operations Center Site :end
Description: Air Operations Center :end

Zone:

Name: General Access :end
Site: Air Operations Center Site :end
//Procedural Security Settings for the AOC Zone

Art: smalloffice.tga :end
HoldsUserAsset: false :end
MaxSecrecyLabel: Secret :end
Static: false :end
MinSecrecyLabel: Unclassified :end
MaxIntegrityLabel: :end
MinIntegrityLabel: :end
ProtectWithACL: false :end
WriteDownPasswords: false :end
LockorLogoff: false :end
PasswordLength: medium :end
PasswordCharacterSet: moderate :end
PasswordChangeFrequency: six :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: false :end
UserBackup: false :end

// END of procedural security component default
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
ModeratePerimeterAlarms: false
Re-enforcedWalls: false
SurveillanceCameras: false
PermitEscortedVisitors: true
VisualPeopleInspection: true
XrayPackages: false
KeyLockOnDoor: false
CipherLockOnDoor: false
ExpensiveIrisScanner: false
ModerateIrisScanner: true
Badges: true
Secrecy: Unclassified
Secrecy: Secret
Integrity: 
Network: LAN 1
Network: LAN 2
Network: LAN 3
ULC: 30 55
LRC: 58 32
Zone:
Name: Reinforced Room
Site: Air Operations Center Site
Art: smallupperzone.tga
HoldsUserAsset: false
MaxSecrecyLabel: Top Secret
MinSecrecyLabel: Secret
MaxIntegrityLabel: false
MinIntegrityLabel: false
ProtectWithACL: false
WriteDownPasswords: false
LockorLogoff: false
PasswordLength: long
PasswordCharacterSet: complex :end
PasswordChangeFrequency: two :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: false :end
UserBackup: false :end
// END of procedural security component default
Receptionist: false :end
GuardAtDoor: false :end
PatrollingGuard: false :end
ProhibitMedia: false :end
ProhibitPhoneDevices: false :end
ExpensivePerimeterAlarms: false :end
ModeratePerimeterAlarms: false :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :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: Top Secret :end
Integrity: :end

Network: LAN 1 :end
Network: LAN 2 :end
Network: LAN 3 :end

ULC: 39 50 :end
LRC: 50 44 :end

Zone:
Name: Server Farm :end
Site: Air Operations Center Site :end

//Proceduaral Security Settings for the Server Farm
Art: offsitezone.tga :end
HoldsUserAsset: false :end
MaxSecrecyLabel: Top Secret :end
MinSecrecyLabel: Unclassified :end
Static: true :end
MaxIntegrityLabel: :end
MinIntegrityLabel: :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 of procedural security component default
Receptionist: true :end
GuardAtDoor: true :end
PatrollingGuard: true :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
ModeratePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
PermitEscortedVisitors: true :end
VisualPeopleInspection: true :end
XrayPackages: true :end
KeyLockOnDoor: true :end
CipherLockOnDoor: true :end
ExpensiveIrisScanner: true :end
ModerateIrisScanner: true :end
Badges: true :end
Secrecy: Top Secret :end
Integrity: :end
Network: S :end
Network: TS :end
Network: U :end
ULC: 94 25 :end
LRC: 103 14 :end

Network: Name: U :end
:end

Network: Name: S :end
:end

Network: Name: TS :end
:end
Network:
  Name: LAN 1 :end
:end

Network:
  Name: LAN 2 :end
:end

Network:
  Name: LAN 3 :end
:end

Department:
  Name: Intel Plans Cell :end
  Name: Logistics Plans Cell :end
  Name: Weather Plans Cell :end
  Name: ATO Production :end
  Name: Current Ops :end
:end

Secrecy:
  Name: Unclassified :end
  Level: 1 :end
  SecrecyValue: 1000 :end
  SecrecyValueChange: 0 :end
  AttackerValue: 45 :end
  AttackerValueChange: 0 :end
  InitialBackGroundCheck: none :end
:end

Secrecy:
  Name: Secret :end
  Level: 2 :end
  SecrecyValue: 4000 :end
  SecrecyValueChange: 0 :end
  AttackerValue: 300 :end
  AttackerValueChange: 0 :end
  InitialBackGroundCheck: Medium :end
:end
Secrecy:

Name: Top Secret
Level: 3
SecrecyValue: 10000
SecrecyValueChange: 0
AttackerValue: 600
AttackerValueChange: 0
InitialBackGroundCheck: High

DACGroups:

Group: WxPlans
InitialBackGroundCheck: none

Group: IntelPlans
InitialBackGroundCheck: Medium

Group: LogPlans
InitialBackGroundCheck: Medium

Group: ATO
InitialBackGroundCheck: Medium

Group: CurrentOps
InitialBackGroundCheck: Medium

Asset:

Name: Intel Feed
Description: This feed is produced via intelligent software agents that employ web crawlers to search various intelligence sources for information on the region of interest. It is the critical source of information used to create the Target List. This feed is the backbone of the AOC. Its classification is Top Secret.
IsInstantiated: true
HasDac: false
Secrecy: Top Secret
Integrity:
DOSMotive: 300
AvailabilityPenalty: 0
AccessList:
  *.IntelPlans YNNN :end // of AccessList:

CostList:
  Access: *.Public :end
  AccessMode: NYNN :end
  Cost: 1000 :end
  AttackerMotive: 10 :end
:end // CostList
:end // Of Intel Feed

Asset:
  Name: Target List :end
  Description: The Target List shows all enemy locations in prioritized order that have strategic importance for
the success of
missions run by the AOC. The targets are prioritized based off of information that is received from the Intel Feed.
  Its classification is Secret.
:end

IsInstantiated: false :end

HasDac: true :end

Secrecy: Secret :end

Integrity: :end

DOSMotive: 0 :end

AvailabilityPenalty: 0 :end

AccessList:
  *.IntelPlans YNNN
  *.ATO YNNN
:end // of AccessList:

CostList:
  Access: *.LogPlans :end
  AccessMode: NYNN :end
  Cost: 1000 :end
  AttackerMotive: 100 :end
:end // CostList
:end // Of Target List

Asset:
  Name: Logistics Resources Feed :end
  Description: This feed updates all logistics information in the operational area. This feed is classified Secret :end

IsInstantiated: true :end

HasDac: false :end

Secrecy: Secret :end

Integrity: :end
Asset:

Name: Logistics Resource List

Description: This is a spreadsheet of resources that will be available for the next 24 hour period of operations. The LRL is compiled from data received over the Logistics Resources Feed. The LRL is classified Secret.

IsInstantiated: false

HasDac: false

Secrecy: Secret

Integrity: 

DOSMotive: 0

AvailabilityPenalty: 0

AccessList:

*.LogPlans YYNN
*.ATO YNNN
:end // of AccessList:

CostList:

Access: *.* :end
AccessMode: YYNN :end
Cost: 100 :end
AttackerMotive: 10 :end
:end // CostList
:end // Of Logistics Resources Server

Asset:

Name: Weather Feed

Description: This feed is a collection of military and civilian weather tracking resources. This feed is Unclassified.

IsInstantiated: true

HasDac: false

Secrecy: Unclassified
Asset:

Name: Area Available List

Description: This listing shows all targets that have suitable weather conditions for the 24 hour period of the ATO. The AAL is based off of information received from the Weather Feed. The AAL is classified Secret.

IsInstantiated: false

HasDac: false

Secrecy: Secret

Integrity: end

DOSMotive: 0

AvailabilityPenalty: 0

AccessList:

*.WxPlans YNNN

CostList:

Access: *.*: end
AccessMode: YYNN: end
Cost: 0: end
AttackerMotive: 0: end

CostList

Access: *.*: end
AccessMode: YYNN: end
Cost: 0: end
AttackerMotive: 0: end

CostList

Asset:

Name: Air Tasking Order

Description: This listing of all missions planned for a 24 hour period. It is based off of inputs from the Target List, the Logistics Resources List, and the Area Available List. The Air Tasking Order is classified Secret.

IsInstantiated: false
HasDac:  false :end

Secrecy: Secret :end

Integrity: :end

DOSMotive:  50 :end

AvailabilityPenalty:  1000 :end

AccessList:
   *.CurrentOps YYNN
   *.ATO YYNN
:end // of AccessList:

CostList:
   Access: *.WxPlans :end
   AccessMode: NYNN :end
   Cost: 1000 :end
   AttackerMotive: 10 :end
:end // CostList
:end // Of Air Tasking Order

Asset:
   Name: Plan B :end

   Description: This is the altered ATO for reading and modification during the 24 flight period :end

   IsInstantiated: true :end

   HasDac:  false :end

   Secrecy: Secret :end

   Integrity: :end

   DOSMotive:  0 :end

   AvailabilityPenalty:  0 :end

   AccessList:
      *.CurrentOps YYNN
   :end // of AccessList:

   CostList:
      Access: *.* :end
      AccessMode: YYNN :end
      Cost: 0 :end
      AttackerMotive: 0 :end
   :end // CostList
:end // Of Plan B

//Beginning of Asset Goals---------------------------------------------------------------

AssetGoal:

   Name: Access Intel Feed :end
Description: Pull down data from the Intel Feed web page using any web browser software. It is critical to the AOC that the person who has this asset goal be able to fulfill it.

Asset:
  Name: Intel Feed
  AccessMode: YNNN

SoftwareType: WEB BROWSER
AvailabilityCostPenalty: 1000

AssetGoal:
  Name: Produce Target List
  Description: Be able to write and organize the prioritized Target List.

Asset:
  Name: Target List
  AccessMode: NYNN

AvailabilityCostPenalty: 500

AssetGoal:
  Name: Access Logistics Feed
  Description: This goal is to access the Logistics Feed.

Asset:
  Name: Logistics Resources Feed
  AccessMode: YNNN

AvailabilityCostPenalty: 70

AssetGoal:
  Name: Produce LRL
  Description: Be able to produce the Logistics Resource List.
Asset:
   Name: Logistics Resource List :end
   AccessMode: NYNN :end
 :end
AvailabilityCostPenalty: 70 :end
:end // of Asset Goal Produce LRL

AssetGoal:
   Name: Access Weather Feed :end
   Description: This goal is to reach out to the Weather Feed and pull down data.
   :end
   Shared: true :end
   Asset:
      Name: Weather Feed :end
      AccessMode: YNNN :end
   :end
   AvailabilityCostPenalty: 70 :end
:end //of Asset Goal Access Weather Feed

AssetGoal:
   Name: Produce AAL :end
   Description: This goal is to produce the Area Available List.
   :end
   Shared: false :end
   Asset:
      Name: Area Available List :end
      AccessMode: NYNN :end
   :end
   AvailabilityCostPenalty: 70 :end
:end // of Asset Goal Produce AAL

AssetGoal:
   Name: Produce ATO :end
   Description: The Air Tasking Order (ATO) is produced and stands as the most important document in the AOC.
   :end
   Shared: false :end
   Asset:
      Name: Air Tasking Order :end
      AccessMode: NYNN :end
   :end
AssetGoal:

Name: Access AAL :end

Description: Access the AAL produced by the Weather Plans Cell. :end

Shared: false :end

Asset:

Name: Area Available List :end
AccessMode: YNNN :end :end

AvailabilityCostPenalty: 70 :end

:end // of Asset Goal Access AAL

AssetGoal:

Name: Access LRL :end

Description: Access the LRL produced by the Logistics Plans Cell. :end

Shared: false :end

Asset:

Name: Logistics Resource List :end
AccessMode: YNNN :end :end

AvailabilityCostPenalty: 70 :end

:end // of Asset Goal Access LRL

AssetGoal:

Name: Access Target List :end

Description: Access the Target List submitted by the Intel Plans Cell. :end

Shared: false :end

Asset:

Name: Target List :end
AccessMode: YNNN :end :end

AvailabilityCostPenalty: 70 :end

:end // of Asset Goal Access Target List

AssetGoal:

Name: Access ATO :end
Description: Be able to read the ATO.

Shared: true

Asset:
- Name: Air Tasking Order
- AccessMode: YYXX

AvailabilityCostPenalty: 70

Asset Goal: Access ATO

Asset Goal: Modify Plan B

Description: Be able to modify the ATO to suit the needs of the battlefield today.

Shared: true

Asset:
- Name: Air Tasking Order
- AccessMode: YYXX

AvailabilityCostPenalty: 70

Asset Goal: Access Intel Feed

TargetUsage: 10
Happiness: 50
Productivity: 90
Trustworthiness: 100
InitialTraining: 95
Happiness: 70
Productivity: 70

User:
Name: Maj Afinidad
Dept: Intel Plans Cell
SecrecyClearance: Top Secret
DACGroups: IntelPlans
DefaultDAC: IntelPlans
Skill: 100 :end
PosIndex: 8 :end
Cost: 5000 :end
Gender: female :end
UserDescription: :end
:end // of User

User:
Name: TSgt Miller :end
Dept: Intel Plans Cell :end
SecrecyClearance: Top Secret :end
DACGroups:
  IntelPlans :end
:end //DACGroups
DefaultDAC: IntelPlans :end
AssetGoal:
  AssetGoalName: Produce Target List :end
  TargetUsage: 80 :end
  Happiness: 50 :end
  Productivity: 50 :end
:end // of AssetGoal
Trustworthiness: 100 :end
InitialTraining: 94 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
PosIndex: 1 :end
Cost: 2000 :end
Gender: male :end
UserDescription: :end
:end // of User

User:
Name: TSgt Johnson :end
Dept: Logistics Plans Cell :end
SecrecyClearance: Secret :end
DACGroups:
  LogPlans :end
:end //DACGroups
DefaultDAC:
  LogPlans :end

AssetGoal:
  AssetGoalName: Access Logistics Feed :end
  TargetUsage: 10 :end
  Happiness: 50 :end
  Productivity: 70 :end
:end // of AssetGoal

AssetGoal:
  AssetGoalName: Produce LRL :end
  TargetUsage: 90 :end
  Happiness: 50 :end
  Productivity: 30 :end
:end // of AssetGoal

Trustworthiness: 100 :end

InitialTraining: 80 :end

Happiness: 60 :end

Productivity: 70 :end

Skill: 100 :end

PosIndex: 2 :end

Cost: 2000 :end

Gender: male :end

UserDescription: :end
:end // of User

User:
  Name: TSgt Lewis :end

Dept: Weather Plans Cell :end

SecrecyClearance: Unclassified :end

DACGroups:
  WxPlans :end
:end //DACGroups

DefaultDAC: WxPlans :end

AssetGoal:
  AssetGoalName: Access Weather Feed :end
  TargetUsage: 100 :end
  Happiness: 100 :end
  Productivity: 100 :end
:end // of AssetGoal

Trustworthiness: 75 :end

InitialTraining: 55 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
PosIndex: 5 :end
Cost: 2000 :end
Gender: male :end
UserDescription: :end
:end // of User

User:
Name: Capt Lisko :end
Dept: Logistics Plans Cell :end
SecrecyClearance: Secret :end
DACGroups:
  WxPlans :end
:end //DACGroups
DefaultDAC: WxPlans :end
AssetGoal:
  AssetGoalName: Produce AAL :end
  TargetUsage: 80 :end
  Happiness: 50 :end
  Productivity: 90 :end
:end // of AssetGoal
AssetGoal:
  AssetGoalName: Access Weather Feed :end
  TargetUsage: 20 :end
  Happiness: 50 :end
  Productivity: 10 :end
:end // of AssetGoal
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
PosIndex: 6 :end
Cost: 4000 :end
Gender: male :end
UserDescription: :end
:end // of User
User:

Name: Lt LaMore :end
Dept: ATO Production Cell :end
Secrecy Clearance: Top Secret :end

DAC Groups:
ATO :end
ATO :end // DAC Groups

Default DAC: ATO :end

Asset Goal:
AssetGoalName: Produce ATO :end
Target Usage: 70 :end
Happiness: 40 :end
Productivity: 40 :end
: end // of Asset Goal

Asset Goal:
AssetGoalName: Access AAL :end
Target Usage: 10 :end
Happiness: 20 :end
Productivity: 20 :end
: end // of Asset Goal

Asset Goal:
AssetGoalName: Access LRL :end
Target Usage: 10 :end
Happiness: 20 :end
Productivity: 20 :end
: end // of Asset Goal

Asset Goal:
AssetGoalName: Access Target List :end
Target Usage: 10 :end
Happiness: 20 :end
Productivity: 20 :end
: end // of Asset Goal

Trustworthiness: 100 : end

Initial Training: 100 : end
Happiness: 70 : end
Productivity: 70 : end
Skill: 100 : end
Pos Index: 3 : end
Cost: 3000 : end
Gender: female : end
User Description: : end

: end // of User
User:

Name: TSgt Samuels
Dept: Current Ops
Secrecy Clearance: Secret
DAC Groups:
  Current Ops
Default DAC: Current Ops
Asset Goal:
  Asset Goal Name: Modify Plan B
  Target Usage: 50
  Happiness: 25
  Productivity: 50
Asset Goal:
  Asset Goal Name: Access ATO
  Target Usage: 50
  Happiness: 25
  Productivity: 50
Trustworthiness: 90
Initial Training: 80
Happiness: 50
Productivity: 70
Skill: 100
Pos Index: 4
Cost: 2000
Gender: male
User Description:

User:

Name: A1C Boxer
Dept: Security
Secrecy Clearance: None
DAC Groups:
  Public
Default DAC: Public
Trustworthiness: 100
User:
  Name: A1C Klinger
  Dept: Security
  Secrecy Clearance: none
  DAC Groups:
    Public
  Default DAC: Public
  Trustworthiness: 100
  Initial Training: 100
  Happiness: 70
  Productivity: 70
  Skill: 100
  Pos Index: 1
  Cost: 500
  Gender: male
  Days Till Available: 0
  User Description: A1C Klinger is a security forces troop

User:
  Name: Randy
  Dept: Tech
  Secrecy Clearance: none
DACGroups:
  Public :end
:end //DACGroups

DefaultDAC: Public :end

Trustworthiness: 100 :end

InitialTraining: 100 :end

Happiness: 70 :end

Productivity: 70 :end

Skill: 90 :end

HISupportSkill: 80 :end

HWSupportSkill: 80 :end

SWSupportSkill: 80 :end

PosIndex: 3 :end

Cost: 2000 :end

Gender: male :end

DaysTillAvailable: 0 :end

UserDescription: Randy is an ex-hacker working for the government :end

:end // of User

User:

Name: Randy, too :end

Dept: Tech :end

SecrecyClearance: none :end

DACGroups:
  Public :end
:end //DACGroups

DefaultDAC: Public :end

Trustworthiness: 100 :end

InitialTraining: 100 :end

Happiness: 70 :end

Productivity: 70 :end

Skill: 99 :end

HISupportSkill: 80 :end

HWSupportSkill: 80 :end

SWSupportSkill: 80 :end

PosIndex: 3 :end

Cost: 2000 :end

Gender: male :end

DaysTillAvailable: 0 :end

UserDescription: Randy is an ex-hacker working for the government :end

:end // of User
SWSupportSkill: 80 :end
PosIndex: 5 :end
Cost: 2000 :end
Gender: male :end
DaysTillAvailable: 0 :end
UserDescription: Randy is an ex-farmer working for the government :end

User:
Name: Randy, as well :end
Dept: Tech :end
SecrecyClearance: none :end
DACGroups:
  Public :end
:end //DACGroups
DefaultDAC: Public :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 99 :end
HISupportSkill: 80 :end
HWSupportSkill: 80 :end
SWSupportSkill: 80 :end
PosIndex: 6 :end
Cost: 2000 :end
Gender: male :end
DaysTillAvailable: 0 :end
UserDescription: Randy is an ex-stock broker working for the government :end
:end // of User

//Components for Intel Plans-----------------------------------------------

Component:
  // Intended machine for Server
Name: Intel Server
IsTemplate: false
Description: Server
AssetProtection: true
HW: Targo Server
Cost: 2000
Resale: 600
Maintenance: 20
Availability: 99
OS: Populos V9 Server
Software: Extortos
Software: Internet Contemplator
RemoteAuthentication: false
AcceptPKICerts: false
UseOneTimePasswordToken: false
UseBiometrics: true
UseTokenPKICerts: false
UseClientPKICerts: false
VPNCert: false
ScanEmailAttachments: true
StripEmailAttachments: true
PasswordComplexity: complex
AutomaticLockLogout: true
SelfAdminister: true
SelfAdministerMAC: false
AdministerSoftwareControl: true
BlockRemovableMedia: true
BlockLocalStorage: true
BrowserSettings: STRICT //switch to loose, normal, strict
EmailSettings: STRICT //switch to loose, normal, strict
UpdatePatches: AUTOMATIC //switch to AsReleased, Routine, Automatic
UpdateAntivirus: AUTOMATIC //Switch to Routine, Automatic
User: :end
PosIndex: 9 :end
Assets: Intel Feed :end
AccessListLocal: :end
AccessListRemote: :end
//TrustedHosts: list :end
UninterruptiblePower: false :end
OffsiteBackup: true :end
CM: WEAK :end // switch to WEAK, MODERATE, STRICT
Network:
    Name: TS :end
    AccessList: :end AccessMode: :end
UserGroupWorld:
    User: :end
    UserMode: :end
    Group: IntelPlans :end
    GroupMode: 777 :end
    WorldMode: NNNN :end
:end
:end
ComponentProceduralSettings:
    HoldsUserAsset: false :end
    MaxSecrecyLabel: Top Secret :end
    MinSecrecyLabel: Top Secret :end
    ProtectWithACL: true :end
    WriteDownPasswords: false :end
    LockorLogoff: true :end
    PasswordLength: long :end
    PasswordCharacterSet: any :end
    PasswordChangeFrequency: two :end
    NoEmailAttachmentExecute: true :end
    NoExternalSoftware: true :end
    NoUseOfModems: false :end
    NoWebMail: true :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: true :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: false :end

:end // Of The Component Procedural Settings
#endif // Component

/components for Logistics Plans ---------------------------------------------------------------
Component:
// Intended machine for Server
  Name: Logistics Server :end
  IsTemplate: false :end
  Description: Workstation :end
  AssetProtection: true :end
  HW: Targo Server :end
  Cost: 2000 :end
  Resale: 600 :end
  Maintenance: 20 :end
  Availability: 99 :end
  OS: Populos V9 Server :end
  Software: Extortos :end
  Software: Internet Contemplator :end
  RemoteAuthentication: false :end
  AcceptPKICerts: false :end
  UseOneTimePasswordToken: false :end
  UseBiometrics: false :end
  UseTokenPKICerts: false :end
  UseClientPKICerts: false :end
  VPNCIent: false :end
  ScanEmailAttachments: false :end
StripEmailAttachments: false

PasswordComplexity: complex

AutomaticLockLogout: true

SelfAdminister: false

SelfAdministerMAC: false

AdministerSoftwareControl: false

BlockRemovableMedia: false

BlockLocalStorage: false

BrowserSettings: LOOSE //switch to loose,normal,strict

EmailSettings: LOOSE //switch to loose,normal,strict

UpdatePatches: NONE //switch to AsReleased,Routine,Automatic

UpdateAntivirus: NONE //Switch to Routine, Automatic

User:

PosIndex: 10

Assets: Logistics Resources Feed

AccessListLocal:

AccessListRemote:

UninterruptiblePower: false

OffsiteBackup: true

CM: WEAK // switch to WEAK, MODERATE, STRICT

Network:

Name: S

AccessList: AccessMode:

UserGroupWorld:

User:

UserMode:

Group: LogPlans

GroupMode: 777

WorldMode: NNNN:

ComponentProceduralSettings:

HoldsUserAsset: false

MaxSecrecyLabel: Secret

MinSecrecyLabel: Secret
//AccessList: :end  AccessMode: :end
ProtectWithACL: true :end
WriteDownPasswords: false :end
LockorLogoff: false :end
PasswordLength: long :end
PasswordCharacterSet: any :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: false :end
NoExternalSoftware: false :end
NoUseOfModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: false :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: false :end

:end // Of The Component Procedural Settings

:end // Component

//Components for Weather Plans -----------------------------------------------

Component:
// Intended machine for Server

Name: Weather Server :end
IsTemplate: false :end
Description: Server :end
AssetProtection: true :end
HW: Targo Server :end
Cost: 2000 :end
Resale: 600 :end
Maintenance: 20 :end
Availability: 99 :end
OS: Populos V9 Server
Software: Extortos
Software: Internet Contemplator
RemoteAuthentication: false
AcceptPKICerts: false
UseOneTimePasswordToken: false
UseBiometrics: false
UseTokenPKICerts: false
UseClientPKICerts: false
VPNClien: false
ScanEmailAttachments: false
StripEmailAttachments: false
PasswordComplexity: complex
AutomaticLockLogout: true
SelfAdminister: false
SelfAdministerMAC: false
AdministerSoftwareControl: false
BlockRemovableMedia: false
BlockLocalStorage: false
BrowserSettings: STRICT
EmailSettings: STRICT
UpdatePatches: AUTOMATIC
UpdateAntivirus: AUTOMATIC
User:
PosIndex: 11
Assets: Weather Feed
AccessListLocal: end
AccessListRemote: end
UninterruptiblePower: false
OffsiteBackup: true
CM: WEAK // switch to WEAK, MODERATE, STRICT
Network:
Name: U :end
AccessList: :end AccessMode: :end

UserGroupWorld:
  User: :end
  UserMode: YYNN :end

  Group: LogPlans :end
  GroupMode: 777 :end

  WorldMode: NNNN :end
  :end
 :end

ComponentProceduralSettings:

  HoldsUserAsset: false :end
  MaxSecrecyLabel: Unclassified :end
  MinSecrecyLabel: Unclassified :end
  ProtectWithACL: true :end
  WriteDownPasswords: false :end
  LockorLogoff: false :end

  PasswordLength: long :end
  PasswordCharacterSet: any :end
  PasswordChangeFrequency: two :end

  NoEmailAttachmentExecute: false :end
  NoExternalSoftware: false :end
  NoUseOfModems: false :end
  NoWebMail: false :end
  NoMediaLeaveZone: true :end
  UpdateAntiVirus: false :end
  ApplyPatches: false :end
  LeaveMachinesOn: true :end
  NoPhysicalModifications: false :end
  UserBackup: false :end

  :end // Of The Component Procedural Settings

  :end // Component

  // Beginning Current Ops Division ------------------------------------------------------------------

  Component:
// Intended machine for Plan B Server

Name: Plan B Server :end
IsTemplate: false :end
Description: Workstation :end
AssetProtection: true :end
HW: Targo Server :end
Cost: 2000 :end
Resale: 600 :end
Maintenance: 20 :end
Availability: 99 :end
OS: Populos V9 Server :end
Software: Extortos :end
Software: Internet Contemplator :end
RemoteAuthentication: false :end
AcceptPKICerts: false :end
UseOneTimePasswordToken: false :end
UseBiometrics: false :end
UseTokenPKICerts: false :end
UseClientPKICerts: false :end
VPNClient: false :end
ScanEmailAttachments: false :end
StripEmailAttachments: false :end
PasswordComplexity: complex :end
AutomaticLockLogout: true :end
SelfAdminister: false :end
SelfAdministerMAC: false :end
AdministerSoftwareControl: false :end
BlockRemovableMedia: false :end
BlockLocalStorage: false :end
BrowserSettings: STRICT :end  //switch to loose,normal,strict
EmailSettings: STRICT :end  //switch to loose,normal,strict
UpdatePatches: AUTOMATIC :end  //switch to AsReleased,Routine,Automatic
UpdateAntivirus: AUTOMATIC :end //Switch to Routine, Automatic

User: :end

PosIndex: 12 :end

Assets: Plan B :end

AccessListLocal: :end

AccessListRemote: :end

UninterruptiblePower: false :end

OffsiteBackup: true :end

CM: STRICT :end // switch to WEAK, MODERATE, STRICT

Network:
   Name: S :end
   AccessList: :end AccessMode: :end

   UserGroupWorld:
       User: :end
       UserMode: :end

       Group: :end
       GroupMode: 777 :end

       WorldMode: NNNN :end
   :end
:end

ComponentProceduralSettings:
   HoldsUserAsset: false :end
   MaxSecrecyLabel: Secret :end
   MinSecrecyLabel: Secret :end
   AccessList: :end AccessMode: :end
   ProtectWithACL: true :end
   WriteDownPasswords: false :end
   LockorLogoff: false :end
   PasswordLength: long :end
   PasswordCharacterSet: any :end
   PasswordChangeFrequency: two :end
   NoEmailAttachmentExecute: false :end
   NoExternalSoftware: false :end
   NoUseOfModems: false :end
NoWebMail: false :end
NoMediaLeaveZone: true :end
UpdateAntiVirus: false :end
ApplyPatches: false :end
LeaveMachinesOn: true :end
NoPhysicalModifications: false :end
UserBackup: false :end

:end // Of The Component Procedural Settings

:end // Component

// Network Device Section ....................................................................................................................................

Component:
// Link Encryptor
    Name: TS Encryptor Offsite :end
    IsTemplate: false :end
    Description: Link Encryptor 2 :end
    AssetProtection: true :end
    HW: Enigma2000 :end
    Cost: 2000 :end
    Resale: 600 :end
    Maintenance: 20 :end
    Availability: 99 :end
    PosIndex: 9 :end
    Network:
        Name: TS :end
    :end // Component

Component:
// Link Encryptor
    Name: S Encryptor Offsite :end
    IsTemplate: false :end
    Description: Link Encryptor 2 :end
    AssetProtection: true :end
    HW: Enigma2000 :end
    Cost: 2000 :end
    Resale: 600 :end
Component:

// Link Encryptor
Name: U Encryptor Offsite :end
IsTemplate: false :end
Description: Link Encryptor 2 :end
AssetProtection: true :end
HW: Enigma2000 :end
Cost: 2000 :end
Resale: 600 :end
Maintenance: 20 :end
Availability: 99 :end
PosIndex: 11 :end
Network:
    Name: U :end
:end // Component

// Component Catalog Section --------------------------------------------------------------------------------------------

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
Component:

Name: Targo Worksaver

IsTemplate: true

Description: Full suite of productivity software, adequate memory and dis.

AssetProtection: true

HW: Targo Worksaver

Cost: 1700

Resale: 200

Maintenance: 100

Availability: 99

OS: Populos V9 Desktop

Component:

Name: Trusted Targo Worksaver

IsTemplate: true

Description: Similar to the Targo Worksaver, but includes the Trusted Populos OS.

AssetProtection: true

HW: Trusted Targo Worksaver

Cost: 2500

Resale: 200

Maintenance: 100

Availability: 99

OS: Trusted Populos Desktop

Component:

Name: The Thin Man

IsTemplate: true

Description: A thin client intended to work with either Gossamer products or Populos Terminal Servers.

AssetProtection: true

HW: The Thin Man

Cost: 900
Resale: 100 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos Embedded V5 :end

Component:
Name: Green Net Client :end
IsTemplate: true :end
Description: A thin client intended to work with Gossamer products. Intended use is to connect to multiple networks of different sensitivity levels :end
AssetProtection: true :end
HW: Green Net Client :end
Cost: 3000 :end
Resale: 1000 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Secure Shade Desktop :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

Component:
Name: Targo Server :end
Component:

Name: Targo Server

IsTemplate: true

Description: Full featured server with the world's most popular operating system.

AssetProtection: true

HW: Targo Server

Cost: 15000

Resale: 5000

Maintenance: 100

Availability: 99

OS: Populos V9 Server

Component:

Name: Blato Server

IsTemplate: true

Description: Full featured server with the world's most popular operating system.

AssetProtection: true

HW: Blato Server

Cost: 15000

Resale: 5000

Maintenance: 100

Availability: 99

OS: Populos V9 Server

Component:

Name: Twist Off Server

IsTemplate: true

Description: Server class machine with the Jar Lid Server O/S

AssetProtection: true

HW: Twist Off Server

Cost: 10000

Resale: 5000

Maintenance: 100
Component:

Name: Green Shade Server
IsTemplate: true
Description: Server class machine with the Secure Shade Server high assurance operating system
AssetProtection: true
HW: Green Shade Server
Cost: 80000
Resale: 20000
Maintenance: 100
Availability: 99
OS: Secure Shade Server

Component:

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

Component:

Name: Web Appliance
IsTemplate: true
Description: Simple web server
AssetProtection: true
HW: Twist Off Server
Software: Populos Web Slave
Cost: 1500
Resale: 2000
Maintenance: 100
Availability: 99
OS: Jar Lid Server

Component:
Name: Populos Internet Slave
IsTemplate: true
Description: Web Server that rules the web.
AssetProtection: true
HW: Blato Server
Software: Populos Web Slave
Cost: 10000
Resale: 2000
Maintenance: 100
Availability: 99
OS: Populos V9 Server

Component:
Name: Bit Flipper VPN
IsTemplate: true
Description: VPN Gateway -- another BitFlipper product
HW: Bit Flipper VPN
Cost: 1500
Resale: 2000
Maintenance: 100
Availability: 99
OS: FlipOS
Component:

Name: Targo Server

IsTemplate: true

Description: Full featured server with the worlds most popular operating system.

AssetProtection: true

HW: Targo Server

Cost: 15000

Resale: 5000

Maintenance: 100

Availability: 99

OS: Populos V9 Server

Component:

Name: Blato Server

IsTemplate: true

Description: Full featured server with the worlds most popular operating system.

AssetProtection: true

HW: Blato Server

Cost: 15000

Resale: 5000

Maintenance: 100

Availability: 99

OS: Populos V9 Server

Component:

Name: Green Shade Server

IsTemplate: true

Description: Server class machine with the Secure Shade Server high assurance operating system

AssetProtection: true

HW: Green Shade Server

Cost: 80000
Component:
Name: Mail Appliance
IsTemplate: true
Description: Simple Email Server.
AssetProtection: true
HW: Targo Server
Software: Do Mail
Cost: 5000
Resale: 2000
Maintenance: 100
Availability: 99
OS: Jar Lid Server

Component:
Name: Bent Line VPN
IsTemplate: true
Description: VPN Gateway Evaluated to EAL4+
HW: Bent Line VPN
Cost: 1500
Resale: 2000
Maintenance: 100
Availability: 99
OS: Populos V8 Server

Component:
Name: Green Shade VPN
IsTemplate: true
Description: VPN Gateway On a Green Shade Core
HW: Green Shade VPN :end
Cost: 1500 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Green Shade Core :end

Component:
Name: Crack This! :end
IsTemplate: true :end
Description: Best Selling VPN Gateway :end
HW: Crack This! :end
Cost: 1500 :end
Resale: 500 :end
Maintenance: 100 :end
Availability: 99 :end
OS: Populos V9 Server :end

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

Component:
Name: Swenthabit :end
IsTemplate: true :end
Description: Vanilla LAN switch

HW: Swenhabit

Cost: 500

Resale: 200

Maintenance: 100

Availability: 99

OS: FlipOS

Component:

Name: Five Inches of Asbestos

IsTemplate: true

Description: Best selling firewall

HW: Five Inches of Asbestos

Cost: 900

Resale: 200

Maintenance: 100

Availability: 99

OS: Populos V9 Desktop

Component:

Name: Bit Flipper Border

IsTemplate: true

Description: Full featured firewall

HW: Bit Flipper Border

Cost: 200

Resale: 100

Maintenance: 100

Availability: 99

OS: Populos V9 Desktop

Component:

Name: Wire Stuff

IsTemplate: true
Component:

Name: High Quality Hub with high reliability

HW: Wire Stuff

Cost: 150

Resale: 100

Maintenance: 100

Availability: 99

Component:

Name: Box with Wires

IsTemplate: true

Description: General purpose hub

HW: Box with Wires

Cost: 90

Resale: 100

Maintenance: 100

Availability: 99

Component:

Name: Paint It Black

IsTemplate: true

Description: Link Encryptor handles most wide area network protocols

HW: Paint It Black

Cost: 290

Resale: 100

Maintenance: 100

Availability: 99

Component:

Name: Enigma2000

IsTemplate: true

Description: Link Encryptor handles most wide area network protocols

HW: Enigma2000
Cost: 290
Resale: 100
Maintenance: 100
Availability: 99

Component:

Name: NightShade
IsTemplate: true
Description: Link Encryptor handles most wide area network protocols
HW: NightShade
Cost: 290
Resale: 100
Maintenance: 100
Availability: 99

OPTIONS:
  UseScenarioCatalogItems: true

Briefing:

Conditions:

//Various Time Conditions
//Time condition for 30 days
Condition:
  Conditionclass: TimeCondition
  Tagname: MonthLong
  Parameter: 720

//Time condition for 1 day
Condition:
  Conditionclass: TimeCondition
  Tagname: OneDay
  Parameter: 24

//Time Condition
Condition:
  Conditionclass: TimeCondition
  Tagname: FiveDays
  Parameter: 120
//Time Condition
Condition:
   Conditionclass: TimeCondition :end
   Tagname: ThreeDays :end
   Parameter: 72 :end
: end //Condition

//Time Condition
Condition:
   Conditionclass: TimeCondition :end
   Tagname: TwoDays :end
   Parameter: 48 :end
: end //Condition

//end Time Conditions

//Lose Condition for 0 cash
Condition:
   Conditionclass: MinCashOnHand :end
   Tagname: Bankrupt :end
   Parameter: 0 :end
   Parameter: 1 :end
: end //Condition

//Lose Condition for Productivity Level to low
Condition:
   Conditionclass: UserProductivity :end
   Tagname: MillerLackofProduct :end
   ConditionText: TSgt Miller :end
   Parameter: 0 :end
   Parameter: 40 :end
: end //Condition

//Lose Condition for Productivity Level to low
Condition:
   Conditionclass: UserProductivity :end
   Tagname: JohnsonLackofProduct :end
   ConditionText: TSgt Johnson :end
   Parameter: 0 :end
   Parameter: 40 :end
: end //Condition

//Lose Condition for Productivity Level to low
Condition:
   Conditionclass: UserProductivity :end
   Tagname: LiskoLackofProduct :end
   ConditionText: Capt Lisko :end
   Parameter: 0 :end
   Parameter: 40 :end
: end //Condition
//Lose Condition for Failed Goal
Condition:

  ConditionClass: UserFailsGoal :end
  TagName: IntelPlansGoalFailure :end
  ConditionText: Maj Afinidad :end
  SecondConditionText: Access Intel Feed :end

:end //Condition

//Lose Condition for Failed Goal
Condition:

  ConditionClass: UserFailsGoal :end
  TagName: LogPlansGoalFailure :end
  ConditionText: TSgt Johnson :end
  SecondConditionText: Access Logistics Feed :end

:end //Condition

//Lose Condition for AssetAttacked
Condition:

  ConditionClass: AssetAttacked :end
  TagName: TSHack :end
  ConditionText: Intel Feed :end
  Parameter: 2 :end
  Parameter: 600 :end
  Parameter: 900 :end

:end //Condition

//Lose Condition for AssetAttacked
Condition:

  ConditionClass: AssetAttacked :end
  TagName: TSHackInternal :end
  ConditionText: Intel Feed :end
  Parameter: 1 :end
  Parameter: 10 :end
  Parameter: 900 :end

:end //Condition

//Win Condition for cash on hand
Condition:

  ConditionClass: MaxCashOnHand :end
  TagName: MostestMoney :end
  Parameter: 10000 :end

:end //condition block

Triggers:

  Trigger:

    TriggerClass: LoseTrigger :end
    TriggerName: GameLostCash :end
FrequencyInDays: 0.5 :end
TriggerText: You are not that well funded (PARAGRAPH) AOC operations have been suspended
because of your inability to manage costs :end
ConditionList: Bankrupt :end
:end //Loss Trigger

Trigger:
TriggerClass: LoseTrigger :end
TriggerName: IntelLostProduce :end
FrequencyInDays: 0.5 :end
FixedDelay: 1.0 :end
RandomDelay: 1.0 :end
TriggerText: Intel Plans was not able to produce the Target List for at least a day, this is
detrimental to the mission of the AOC :end
ConditionList: MillerLackofProduct :end
:end //Loss Trigger

Trigger:
TriggerClass: LoseTrigger :end
TriggerName: LogLostProduce :end
FrequencyInDays: 0.5 :end
FixedDelay: 2.0 :end
RandomDelay: 1.0 :end
TriggerText: Logistics Plans was not able to produce the Logistics Resource List for at least 2 days,
this is unacceptable and you have been transferred to an Alaskan Weather Station :end
ConditionList: JohnsonLackofProduct :end
:end //Loss Trigger

Trigger:
TriggerClass: LoseTrigger :end
TriggerName: WxLostProduce :end
FrequencyInDays: 0.5 :end
FixedDelay: 3.0 :end
RandomDelay: 1.0 :end
TriggerText: Weather Plans was not able to produce the Area Available List for at least 3 days, this
incompetence has cost lives and you have been removed from your position :end
ConditionList: LiskoLackofProduct :end
:end //Loss Trigger

Trigger:
TriggerClass: BudgetTrigger :end
TriggerName: BudgetReallocation :end
FrequencyInDays: 0.4 :end
RandomDelay: 15.0 :end
TriggerText: A portion of your budget has been reallocated to support the fight against Canada :end
Parameter: -8000 :end
ConditionList: ThreeDays :end
:end //Budget Trigger

Trigger:
TriggerClass: MessageTrigger :end
TriggerName: FailedIntelGoal :end
FrequencyInDays: 0.5 :end
TriggerText: Maj Afinidad is not able to fulfill her asset goal, make sure she has the means to her
goal :end
ConditionList: IntelPlansGoalFailure :end
:end //Loss Trigger

Trigger:
TriggerClass: MessageTrigger :end
TriggerName: FailedLogGoal :end
FrequencyInDays: 0.5 :end
TriggerText: You are not that well funded (PARAGRAPH) AOC operations have been suspended
because of your inability to manage costs :end
ConditionList: Bankrupt :end
:end //Loss Trigger
Frequency In Days: 0.9
Trigger Text: TSgt Johnson is not able to fulfill his asset goal to read the logistics feed, make sure he has the means to his goal.
Condition List: Log Plans Goal Failure

Trigger:
  Trigger Class: Lose Trigger
  Trigger Name: Lose by Attack Success
  Frequency In Days: 0.5
  Trigger Text: The Intel Feed was compromised by an external attacker, you are an idiot.
Condition List: TSHack

Trigger:
  Trigger Class: Lose Trigger
  Trigger Name: Lose by Attack Success 2
  Frequency In Days: 0.5
  Trigger Text: The Intel Feed was compromised by an internal attacker, you are betrayed.
Condition List: TSHack Internal

Trigger:
  Trigger Class: Win Trigger
  Trigger Name: Win Cash Over Time
  Frequency In Days: 0.5
  Trigger Text: You have operated for 30 days, you have achieved victory
Condition List: Month Long

Trigger:
  Trigger Class: Ticker Trigger
  Trigger Name: ATO Published
  Frequency In Days: 1.0
  Trigger Text: The ATO has been published
Parameter: 9999
Condition List: One Day

:End //of Triggers

:End Of File

C. AOCPLAYABLEGAME.SDF

// Game generated save game file
// Real Time: Sun May 30 14:50:45 2004
// Game Time: Jan 6 06:22 pm
//

Organization:
  Name: AOC
  Title: Air Operations Center
  Use Work Offsite Office: False
  Internet: False
  Use Small Office: True
  Start Money: 9030
  Budget: 10000
  Start Month: 1
  Start Day: 6
  Start Hour: 18
**StartMinute:** 22
**UseWorkOffsiteOffice:** False
**WorkSpaceFile:** WorkSpaceAOC.txt
**ProfitSharing:** 75

### Site
- **Name:** Air Operations Center Site
- **Description:** Air Operations Center

### Camera
- **ViewCenterX:** 45
- **ViewCenterY:** 41
- **ViewAmountBack:** 70
- **ViewAmountUp:** 37

### Network
- **Name:** U
- **Name:** S
- **Name:** TS
- **Name:** LAN 1
- **Name:** LAN 2
- **Name:** LAN 3

### Zone
- **Name:** General Access
- **Site:** Air Operations Center Site
- **Art:** smalloffice.tga
- **Description:**

#### Start Default Component Settings
- **PasswordLength:** Medium
- **PasswordCharacterSet:** Moderate
- **PasswordChangeFrequency:** six
- **MaxSecrecyLabel:** Secret
- **MinSecrecyLabel:** Unclassified
- **MaxIntegrityLabel:**
- **MinIntegrityLabel:**

#### Start Zone Security Settings
- **Receptionist:** true
- **GuardAtDoor:** true
- **PatrollingGuard:** true
- **VisualPeopleInspection:** true
- **KeyLockOnDoor:** true

---

139
CipherLockOnDoor: true :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ModeratePerimeterAlarms: true :end
ExpensiveIrisScanner: true :end
ModerateIrisScanner: true :end
Badges: true :end
PermitEscortedVisitors: true :end
PermittedUsers: *.WxPlans :end
PermittedUsers: *.LogPlans :end
PermittedUsers: *.ATO :end
Secrecy: Unclassified :end
Secrecy: Secret :end
// End Zone Security Settings
ULC: 30 55 :end
LRC: 58 32 :end
:end // Zone Block

Zone:
  Name: Reinforced Room :end
  Site: Air Operations Center Site :end
  Art: smallupperzone.tga :end
  Description: :end
  // Start Default Component Settings
  PasswordLength: Long :end
  PasswordCharacterSet: Complex :end
  PasswordChangeFrequency: two :end
  MaxSecrecyLabel: Top Secret :end
  MinSecrecyLabel: Secret :end
  MaxIntegrityLabel: :end
  MinIntegrityLabel: :end
  // End Default Component Settings
  // Start Zone Security Settings
  Receptionist: true :end
  GuardAtDoor: true :end
  PatrollingGuard: true :end
  VisualPeopleInspection: true :end
  KeyLockOnDoor: true :end
  CipherLockOnDoor: true :end
  ProhibitMedia: true :end
  ProhibitPhoneDevices: true :end
  Re-enforcedWalls: true :end
  SurveillanceCameras: true :end
  PermittedUsers: Maj Afinidad :end
  PermittedUsers: *.IntelPlans :end
  Secrecy: Top Secret :end
  // End Zone Security Settings
  ULC: 39 50 :end
  LRC: 50 44 :end
:end // Zone Block

Zone:
  Name: Server Farm :end
  Site: Air Operations Center Site :end
  Art: offsitezone.tga :end
  Description: :end
  Static: true :end
  // Start Default Component Settings
  ProtectWithACL: true :end
  LockorLogoff: true :end
  PasswordLength: Long :end
  PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoUseOfModems: true :end
NoMediaLeaveZone: true :end
NoWebMail: true :end
ApplyPatches: true :end
LeaveMachinesOn: true :end
NoPhysicalModifications: true :end
UpdateAntivirus: Regular :end
MaxSecrecyLabel: Top Secret :end
MinSecrecyLabel: Unclassified :end
MaxIntegrityLabel: :end
MinIntegrityLabel: :end
// End Default Component Settings
// Start Zone Security Settings
Receptionist: true :end
GuardAtDoor: true :end
PatrollingGuard: true :end
VisualPeopleInspection: true :end
KeyLockOnDoor: true :end
CipherLockOnDoor: true :end
ProhibitMedia: true :end
ProhibitPhoneDevices: true :end
ExpensivePerimeterAlarms: true :end
ModeratePerimeterAlarms: true :end
Re-enforcedWalls: true :end
SurveillanceCameras: true :end
XRayPackages: true :end
ExpensiveIrisScanner: true :end
ModerateIrisScanner: true :end
Badges: true :end
PermitEscortedVisitors: true :end
Secrecy: Top Secret :end
// End Zone Security Settings
ULC: 94 25 :end
LRC: 103 14 :end
:end // Zone Block

Department:
  Name: Current Ops :end
:end

Secrecy:
  Name: Unclassified :end
  Level: 1 :end
  Category: 0 :end
  SecrecyValue: 1000 :end
  SecrecyValueChange: 0 :end
  AttackerValue: 45 :end
  AttackerValueChange: 0 :end
  InitialBackGroundCheck: Medium :end
:end // Label Block

Secrecy:
  Name: Secret :end
  Level: 2 :end
  Category: 0 :end
  SecrecyValue: 4000 :end
  SecrecyValueChange: 0 :end
  AttackerValue: 300 :end
  AttackerValueChange: 0 :end
Initia1 BackGround Check: Medium :end :end // Label Block

Secrecy:
  Name: Top Secret :end
  Level: 3 :end
  Category: 0 :end
  SecrecyValue: 10000 :end
  SecrecyValueChange: 0 :end
  AttackerValue: 600 :end
  AttackerValueChange: 0 :end
Initia1 BackGround Check: High :end :end // Label Block

DACGroups:
  Group: WxPlans :end
  Initial BackGround Check: None :end
  Group: IntelPlans :end
  Initial BackGround Check: Medium :end
  Group: LogPlans :end
  Initial BackGround Check: Medium :end
  Group: ATO :end
  Initial BackGround Check: Medium :end
  Group: CurrentOps :end
  Initial BackGround Check: Medium :end :end // DAC Groups

Asset:
  Name: Intel Feed :end
  Description: This feed is produced via intelligent software agents that employ web crawlers to search various intelligence sources for information on the region of interest. It is the critical source of information used to create the Target List. This feed is the backbone of the AOC. Its classification is Top Secret. :end
  IsInstantiated: True :end
  Secrecy: Top Secret :end
  DOSMotive: 300 :end
  AvailabilityPenalty: 0 :end
  AccessList:
    *.IntelPlans YNNN :end // Accesslist
  CostList:
    Access: *.Public :end
    AccessMode: YYYY :end
    Cost: 0 :end
    AttackerMotive: 0 :end :end // CostList
// Start Asset attacked history
  AttackHistory: 0 -1 -1 :end
  AttackHistory: 1 -1 -1 :end
  AttackHistory: 2 -1 -1 :end
  AttackHistory: 3 -1 -1 :end
  AttackHistory: 4 -1 -1 :end
  AttackHistory: 5 -1 -1 :end
  AttackHistory: 6 -1 -1 :end
// End Asset attacked history :end // Asset

Asset:
  Name: Target List :end
  Description: The Target List shows all enemy locations in prioritized order that of strategic importance for the success of missions run by the AOC. The targets are prioritized based on information that is received from the Intel Feed. Its classification is Secret. :end
  IsInstantiated: True :end
Asset:

Name: Logistics Resources Feed

Description: This feed updates all logistics information in the operational area. This feed is classified Secret.

IsInstantiated: True

Secrecy: Secret

DOSMotive: 0

AvailabilityPenalty: 0

AccessList:

*.IntelPlans YYNN
*.ATO YNNN

CostList:

Access: *.LogPlans
AccessMode: YYNN
Cost: 100
AttackerMotive: 100

// Start Asset attacked history

AttackHistory: 0 -1 -1
AttackHistory: 1 -1 -1
AttackHistory: 2 -1 -1
AttackHistory: 3 -1 -1
AttackHistory: 4 -1 -1
AttackHistory: 5 -1 -1
AttackHistory: 6 -1 -1

// End Asset attacked history

:end // Asset

Asset:

Name: Logistics Resource List

Description: This is a spreadsheet of resources that will be available for the next 24 hour period of operations. The LRL is compiled from data received over the Logistics Resources Feed. The LRL is classified Secret.

IsInstantiated: True

Secrecy: Secret

DOSMotive: 0

AvailabilityPenalty: 0

AccessList:

*.LogPlans YYNN
*.ATO YNNN

CostList:

Access: *.Public
AccessMode: YYNN
Cost: 100
AttackerMotive: 10

// Start Asset attacked history

AttackHistory: 0 -1 -1
AttackHistory: 1 -1 -1
AttackHistory: 2 -1 -1
AttackHistory: 3 -1 -1
AttackHistory: 4 -1 -1
AttackHistory: 5 -1 -1
AttackHistory: 6 -1 -1

// End Asset attacked history

:end // Asset
Asset:
   Name: Weather Feed :end
   Description: This feed is a collection of military and civilian weather tracking resources. This feed is Unclassified. :end

Asset:
   Name: Area Available List :end
   Description: This listing shows all targets that have suitable weather conditions for the 24 hour period of the ATO. The AAL is based off of information received from the Weather Feed. The AAL is classified Secret. :end
Asset:
Name: Air Tasking Order :end
Description: This listing of all missions planned for a 24 hour period. It is based off of inputs from the Target List, the Logistics Resources List, and the Area Available List. The Air Tasking Order is classified Secret. :end
IsInstantiated: True :end
Secrecy: Secret :end
DOSMotive: 50 :end
AvailabilityPenalty: 1000 :end
AccessList:
*.ATO YYNN
*.CurrentOps YYNN :end //Accesslist
CostList:
Access: *.WxPlans :end
AccessMode: NYNN :end
Cost: 1000 :end
AttackerMotive: 10 :end :end //CostList
// Start Asset attacked history
AttackHistory: 0 -1 -1 :end
AttackHistory: 1 -1 -1 :end
AttackHistory: 2 -1 -1 :end
AttackHistory: 3 -1 -1 :end
AttackHistory: 4 -1 -1 :end
AttackHistory: 5 -1 -1 :end
AttackHistory: 6 -1 -1 :end
// End Asset attacked history
:end // Asset

Asset:
Name: Plan B :end
Description: This is the altered ATO for reading and modification during the 24 flight period :end
IsInstantiated: True :end
Secrecy: Secret :end
DOSMotive: 0 :end
AvailabilityPenalty: 0 :end
AccessList:
*.CurrentOps YYNN :end //Accesslist
CostList:
Access: *.Public :end
AccessMode: YYNN :end
Cost: 0 :end
AttackerMotive: 0 :end :end //CostList
// Start Asset attacked history
AttackHistory: 0 -1 -1 :end
AttackHistory: 1 -1 -1 :end
AttackHistory: 2 -1 -1 :end
AttackHistory: 3 -1 -1 :end
AttackHistory: 4 -1 -1 :end
AttackHistory: 5 -1 -1 :end
AttackHistory: 6 -1 -1 :end
// End Asset attacked history
:end // Asset
AssetGoal:
Name: Access Intel Feed :end
Description: Pull down data from the Intel Feed web page using any web browser software. It is critical to the AOC that the person who has this asset goal be able to fulfill it. :end
Asset:
  Name: Intel Feed :end
  AccessMode: YNNN :end
  AvailabilityCostPenalty: 1000 :end
:end // Asset Goal

AssetGoal:
Name: Produce Target List :end
Description: Be able to write and organize the prioritized Target List. :end
Asset:
  Name: Target List :end
  AccessMode: NYNN :end
  AvailabilityCostPenalty: 500 :end
:end // Asset Goal

AssetGoal:
Name: Access Logistics Feed :end
Description: This goal is to access the Logistics Feed. :end
Asset:
  Name: Logistics Resources Feed :end
  AccessMode: YNNN :end
  AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
Name: Produce LRL :end
Description: Be able to produce the Logistics Resource List. :end
Asset:
  Name: Logistics Resource List :end
  AccessMode: NYNN :end
  AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
Name: Access Weather Feed :end
Description: This goal is to reach out to the Weather Feed and pull down data. :end
Asset:
  Name: Weather Feed :end
  AccessMode: YNNN :end
  AvailabilityCostPenalty: 70 :end
:end // Asset Goal

AssetGoal:
Name: Produce AAL :end
Description: This goal is to produce the Area Available List. :end
Asset:
  Name: Area Available List :end
  AccessMode: NYNN :end :end
  AvailabilityCostPenalty: 70 :end :end // Asset Goal

AssetGoal:
  Name: Produce ATO :end
  Description: The Air Tasking Order (ATO) is produced and stands as the most important document in the AOC.
  Asset:
    Name: Air Tasking Order :end
    AccessMode: NYNN :end :end
    AvailabilityCostPenalty: 70 :end :end // Asset Goal

AssetGoal:
  Name: Access AAL :end
  Description: Access the AAL produced by the Weather Plans Cell.
  Asset:
    Name: Area Available List :end
    AccessMode: YNNN :end :end
    AvailabilityCostPenalty: 70 :end :end // Asset Goal

AssetGoal:
  Name: Access LRL :end
  Description: Access the LRL produced by the Logistics Plans Cell.
  Asset:
    Name: Logistics Resource List :end
    AccessMode: YNNN :end :end
    AvailabilityCostPenalty: 70 :end :end // Asset Goal

AssetGoal:
  Name: Access Target List :end
  Description: Access the Target List submitted by the Intel Plans Cell.
  Asset:
    Name: Target List :end
    AccessMode: YNNN :end :end
    AvailabilityCostPenalty: 70 :end :end // Asset Goal

AssetGoal:
  Name: Access ATO :end
  Description: Be able to read the ATO.
  Asset:
    Name: Air Tasking Order :end
    AccessMode: YYNN :end :end
    AvailabilityCostPenalty: 70 :end :end // Asset Goal

AssetGoal:
  Name: Modify Plan B :end
  Description: Be able to modify the ATO to suit the needs of the battlefield today.
  Asset:
Name: Air Tasking Order :end
AccessMode: YYNN :end :end
AvailabilityCostPenalty: 70 :end :end // Asset Goal

User:
Name: Maj Afinidad :end
Dept: Intel Plans Cell :end
SecrecyClearance: Top Secret :end
DACGroups:
  Public :end
  IntelPlans :end :end
AssetGoal:
  AssetGoalName: Access Intel Feed :end
  TargetUsage: 10 :end
  Happiness: 50 :end
  Productivity: 86 :end :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 8 :end
Cost: 5000 :end
Gender: female :end
UserDescription: :end :end // User

User:
Name: TSgt Miller :end
Dept: Intel Plans Cell :end
SecrecyClearance: Top Secret :end
DACGroups:
  Public :end
  IntelPlans :end :end
AssetGoal:
  AssetGoalName: Produce Target List :end
  TargetUsage: 80 :end
  Happiness: 50 :end
  Productivity: 48 :end :end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 1 :end
Cost: 2000 :end
Gender: male :end
UserDescription: :end :end // User
User:
   Name: TSgt Johnson :end
   Dept: Logistics Plans Cell :end
   SecrecyClearance: Secret :end
   DACGroups:
      Public :end
      LogPlans :end
   :end
   AssetGoal:
      AssetGoalName: Access Logistics Feed :end
      TargetUsage: 10 :end
      Happiness: 50 :end
      Productivity: 67 :end
   :end
   AssetGoal:
      AssetGoalName: Produce LRL :end
      TargetUsage: 90 :end
      Happiness: 50 :end
      Productivity: 29 :end
   :end
   Trustworthiness: 100 :end
   InitialTraining: 100 :end
   Happiness: 60 :end
   Productivity: 70 :end
   Skill: 100 :end
   HISupportSkill: 0 :end
   HWSupportSkill: 0 :end
   SWSupportSkill: 0 :end
   PosIndex: 2 :end
   Cost: 2000 :end
   Gender: male :end
   UserDescription: :end
:end // User

User:
   Name: TSgt Lewis :end
   Dept: Weather Plans Cell :end
   SecrecyClearance: Unclassified :end
   DACGroups:
      Public :end
      WxPlans :end
   :end
   AssetGoal:
      AssetGoalName: Access Weather Feed :end
      TargetUsage: 100 :end
      Happiness: 100 :end
      Productivity: 95 :end
   :end
   Trustworthiness: 75 :end
   InitialTraining: 90 :end
   Happiness: 70 :end
   Productivity: 70 :end
   Skill: 100 :end
   HISupportSkill: 0 :end
   HWSupportSkill: 0 :end
   SWSupportSkill: 0 :end
   PosIndex: 5 :end
   Cost: 2000 :end
   Gender: male :end
   UserDescription: :end
:end // User
User:
Name: Capt Lisko :end
Dept: Logistics Plans Cell :end
SecrecyClearance: Secret :end
DACGroups:
  Public :end
  WxPlans :end
:end
AssetGoal:
  AssetGoalName: Access Weather Feed :end
  TargetUsage: 20 :end
  Happiness: 50 :end
  Productivity: 10 :end
:end
AssetGoal:
  AssetGoalName: Produce AAL :end
  TargetUsage: 80 :end
  Happiness: 50 :end
  Productivity: 86 :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 6 :end
Cost: 4000 :end
Gender: male :end
UserDescription: :end
:end // User

User:
Name: Lt LaMore :end
Dept: ATO Production Cell :end
SecrecyClearance: Top Secret :end
DACGroups:
  Public :end
  ATO :end
:end
AssetGoal:
  AssetGoalName: Produce ATO :end
  TargetUsage: 70 :end
  Happiness: 40 :end
  Productivity: 38 :end
:end
AssetGoal:
  AssetGoalName: Access AAL :end
  TargetUsage: 10 :end
  Happiness: 20 :end
  Productivity: 19 :end
:end
AssetGoal:
  AssetGoalName: Access LRL :end
  TargetUsage: 10 :end
  Happiness: 20 :end
  Productivity: 19 :end
:end
AssetGoal:
  AssetGoalName: Access Target List :end
TargetUsage: 10 :end
Happiness: 20 :end
Productivity: 19 :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 3 :end
Cost: 3000 :end
Gender: female :end
UserDescription: :end
:end // User

User:
Name: TSgt Samuels :end
Dept: Current Ops :end
SecrecyClearance: Secret :end
DACGroups:
  Public :end
  CurrentOps :end
:end
AssetGoal:
  AssetGoalName: Access ATO :end
  TargetUsage: 50 :end
  Happiness: 25 :end
  Productivity: 48 :end
:end
AssetGoal:
  AssetGoalName: Modify Plan B :end
  TargetUsage: 50 :end
  Happiness: 25 :end
  Productivity: 48 :end
:end
Trustworthiness: 90 :end
InitialTraining: 100 :end
Happiness: 50 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 4 :end
Cost: 2000 :end
Gender: male :end
UserDescription: :end
:end // User

User:
Name: Randy, as well :end
Dept: Tech :end
DACGroups:
  Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 99 :end
HISupportSkill: 80 :end
HWSupportSkill: 80 :end
SWSupportSkill: 80 :end
PosIndex: 6 :end
Cost: 2000 :end
Gender: male :end
UserDescription: Randy is an ex-stock broker working for the government :end
:end // User

User:
Name: A1C Boxer :end
Dept: Security :end
DACGroups:
  Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 0 :end
Cost: 2000 :end
Gender: male :end
UserDescription: A1C Boxer is a security forces troop :end
:end // User

User:
Name: A1C Klinger :end
Dept: Security :end
DACGroups:
  Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 100 :end
HISupportSkill: 0 :end
HWSupportSkill: 0 :end
SWSupportSkill: 0 :end
PosIndex: 1 :end
Cost: 500 :end
Gender: male :end
UserDescription: A1C Klinger is a security forces troop :end
:end // User

User:
Name: Randy :end
Dept: Tech :end
DACGroups:
  Public :end
:end
Trustworthiness: 100 :end
InitialTraining: 100 :end
Happiness: 70 :end
Productivity: 70 :end
Skill: 90 :end
HISupportSkill: 80 :end
User:
Name: Randy, too
Dept: Tech
DACGroups:
  Public
Trustworthiness: 100
InitialTraining: 100
Happiness: 70
Productivity: 70
Skill: 99
HISupportSkill: 80
HWSupportSkill: 80
SWSupportSkill: 80
PosIndex: 5
Cost: 2000
Gender: male
UserDescription: Randy is an ex-farmer working for the government
DaysTillAvailable: 0

Component:
Name: Intel Server
IsTemplate: false
AssetProtection: True
HW: Targo Server
Static: false
Availability: 100
Resale: 600
OS: Populos V9 Server
Software: Internet Contemplator
Software: Extortos
Software: GrayBird
UseBiometrics: true
ScanEmailAttachments: true
StripEmailAttachments: true
AutomaticLockLogout: true
SelfAdminister: true
AdministerSoftwareControl: true
BlockRemovableMedia: true
BlockLocalStorage: true
BrowserSettings: Strict
EmailSettings: Strict
UpdatePatches: Automatic
ConfigUpdateAntivirus: Automatic
CM: Weak
PosIndex: 9
Assets: Intel Feed
AccessListRemote: Maj Afinidad
Network:
  Name: TS
  AccessList: *.Public
  AccessMode: YYYY

User Description: Randy is an ex-hacker working for the government
DaysTillAvailable: 0

User:
Name: Randy, too
Dept: Tech
DACGroups:
  Public
Trustworthiness: 100
InitialTraining: 100
Happiness: 70
Productivity: 70
Skill: 99
HISupportSkill: 80
HWSupportSkill: 80
SWSupportSkill: 80
PosIndex: 5
Cost: 2000
Gender: male
UserDescription: Randy is an ex-farmer working for the government
DaysTillAvailable: 0

Component:
Name: Intel Server
IsTemplate: false
AssetProtection: True
HW: Targo Server
Static: false
Availability: 100
Resale: 600
OS: Populos V9 Server
Software: Internet Contemplator
Software: Extortos
Software: GrayBird
UseBiometrics: true
ScanEmailAttachments: true
StripEmailAttachments: true
AutomaticLockLogout: true
SelfAdminister: true
AdministerSoftwareControl: true
BlockRemovableMedia: true
BlockLocalStorage: true
BrowserSettings: Strict
EmailSettings: Strict
UpdatePatches: Automatic
ConfigUpdateAntivirus: Automatic
CM: Weak
PosIndex: 9
Assets: Intel Feed
AccessListRemote: Maj Afinidad
Network:
  Name: TS
  AccessList: *.Public
  AccessMode: YYYY
ComponentProceduralSettings:
ProtectWithACL: true :end
LockorLogoff: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoEmailAttachmentExecute: true :end
NoExternalSoftware: true :end
NoMediaLeaveZone: true :end
NoWebMail: true :end
LeaveMachinesOn: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
  Name: Logistics Server :end
  IsTemplate: false :end
  AssetProtection: True :end
  HW: Targo Server :end
  Static: false :end
  Availability: 100 :end
  Resale: 600 :end
  OS: Populos V9 Server :end
  Software: Internet Contemplator :end
  Software: Extortos :end
  Software: POP.Mumo Virus :end
  Software: POP.Sling Virus :end
  AutomaticLockLogout: true :end
  BrowserSettings: Loose :end
  EmailSettings: Loose :end
  CM: Weak :end
  PosIndex: 10 :end
  Assets: Logistics Resources Feed :end
  AccessListRemote: TSgt Johnson :end
  Network:
    Name: S :end
:end // of network description
ComponentProceduralSettings:
ProtectWithACL: true :end
PasswordLength: Long :end
PasswordCharacterSet: Any :end
PasswordChangeFrequency: two :end
NoMediaLeaveZone: true :end
LeaveMachinesOn: true :end
:end // ComponentProceduralSettings
:end // Component

Component:
  Name: Weather Server :end
  IsTemplate: false :end
  AssetProtection: True :end
  HW: Targo Server :end
  Static: false :end
  Availability: 100 :end
  Resale: 600 :end
  OS: Populos V9 Server :end
  Software: Internet Contemplator :end
  Software: Extortos :end
  Software: POP.TuPEG Virus :end
  Software: POP.Mumo Virus :end
  Software: POP.Sling Virus :end
AutomaticLockLogout: true :end
BrowserSettings: Strict :end
EmailSettings: Strict :end
UpdatePatches: Automatic :end
ConfigUpdateAntivirus: Automatic :end
CM: Weak :end
PosIndex: 11 :end
Assets: Weather Feed :end
AccessListRemote: TSgt Lewis :end
AccessListRemote: Capt Lisko :end
Network:
   Name: U :end
ComponentProceduralSettings:
   ProtectWithACL: true :end
   PasswordLength: Long :end
   PasswordCharacterSet: Any :end
   PasswordChangeFrequency: two :end
   NoMediaLeaveZone: true :end
   LeaveMachinesOn: true :end
   :end // ComponentProceduralSettings
:end // Component

Component:
   Name: Plan B Server :end
   IsTemplate: false :end
   AssetProtection: True :end
   HW: Targo Server :end
   Static: false :end
   Availability: 100 :end
   Resale: 600 :end
   OS: Populos V9 Server :end
   Software: Internet Contemplator :end
   Software: Extortos :end
   Software: Defiler :end
   Software: GrayBird :end
   Software: Aladinz :end
   AutomaticLockLogout: true :end
   BrowserSettings: Strict :end
   EmailSettings: Strict :end
   UpdatePatches: Automatic :end
   ConfigUpdateAntivirus: Automatic :end
   CM: Strong :end
   PosIndex: 12 :end
   Assets: Plan B :end
   Network:
      Name: S :end
      :end // of network description
   ComponentProceduralSettings:
      ProtectWithACL: true :end
      PasswordLength: Long :end
      PasswordCharacterSet: Any :end
      PasswordChangeFrequency: two :end
      NoMediaLeaveZone: true :end
      LeaveMachinesOn: true :end
      :end // ComponentProceduralSettings
   :end // Component

Component:
   Name: Blato Desktop Select_6 :end
Component:
Name: Blato Desktop Select_7 :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 100 :end
Resale: 200 :end
OS: Populos V9 Desktop :end
Software: Internet Contemplator :end
Software: GrayBird :end
User: Maj Afinidad :end
PosIndex: 8 :end
AccessListLocal: Maj Afinidad :end
AccessListRemote: Maj Afinidad :end
Network:
  Name: LAN 1 :end
ComponentProceduralSettings:
PasswordLength: Long :end
PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end :end // ComponentProceduralSettings
end // Component

Component:
Name: Blato Desktop Select_7 :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 100 :end
Resale: 200 :end
OS: Populos V9 Desktop :end
Software: GrayBird :end
Software: POP.Sling Virus :end
User: TSgt Miller :end
PosIndex: 1 :end
Assets: Target List :end
AccessListLocal: TSgt Miller :end
AccessListRemote: TSgt Miller :end
AccessListRemote: Lt LaMore :end
Network:
  Name: LAN 2 :end
ComponentProceduralSettings:
PasswordLength: Long :end
PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end :end // ComponentProceduralSettings
end // Component

Component:
Name: Blato Desktop Select_8 :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 100 :end
Resale: 200 :end
OS: Populos V9 Desktop :end
Software: Defiler :end
Software: GrayBird :end
User: TSgt Miller :end
PosIndex: 1 :end
Assets: Target List :end
AccessListLocal: TSgt Miller :end
AccessListRemote: TSgt Miller :end
AccessListRemote: Lt LaMore :end
Network:
  Name: LAN 1 :end
ComponentProceduralSettings:
PasswordLength: Long :end
PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end :end // ComponentProceduralSettings
end // Component

Component:
Name: Blato Desktop Select_8 :end
IsTemplate: false :end
AssetProtection: True :end
HW: Blato Desktop Select :end
Static: false :end
Availability: 100 :end
Resale: 200 :end
OS: Populos V9 Desktop :end
Software: Defiler :end
Software: GrayBird :end
User: TSgt Miller :end
PosIndex: 1 :end
Assets: Target List :end
AccessListLocal: TSgt Miller :end
AccessListRemote: TSgt Miller :end
AccessListRemote: Lt LaMore :end
Network:
  Name: LAN 2 :end
ComponentProceduralSettings:
PasswordLength: Long :end
PasswordCharacterSet: Complex :end
PasswordChangeFrequency: two :end :end // ComponentProceduralSettings
end // Component
Software: POP.Sling Virus :end
User: TSgt Lewis :end
PosIndex: 5 :end
AccessListLocal: TSgt Lewis :end
AccessListRemote: TSgt Lewis :end
Network:
   Name: U :end
ComponentProceduralSettings:
   PasswordLength: Medium :end
   PasswordCharacterSet: Moderate :end
   PasswordChangeFrequency: six :end :end // ComponentProceduralSettings
:end // Component

Component:
   Name: Blato Desktop Select_9 :end
   IsTemplate: false :end
   AssetProtection: True :end
   HW: Blato Desktop Select :end
   Static: false :end
   Availability: 100 :end
   Resale: 200 :end
   OS: Populos V9 Desktop :end
   Software: Defiler :end
   Software: POP.Sling Virus :end
   User: Capt Lisko :end
   PosIndex: 6 :end
   AccessListLocal: Capt Lisko :end
   AccessListRemote: Capt Lisko :end
   AccessListRemote: Lt LaMore :end
   Network:
      Name: U :end
      ComponentProceduralSettings:
      PasswordLength: Medium :end
      PasswordCharacterSet: Moderate :end
      PasswordChangeFrequency: six :end :end // ComponentProceduralSettings
   :end // Component

Component:
   Name: Blato Desktop Select_10 :end
   IsTemplate: false :end
   AssetProtection: True :end
   HW: Blato Desktop Select :end
   Static: false :end
   Availability: 100 :end
   Resale: 200 :end
   OS: Populos V9 Desktop :end
   Software: Aladinz :end
   Software: POP.Mumo Virus :end
   Software: POP.Sling Virus :end
   EnforcePasswordPolicy: true :end
   DetailedLogging: true :end
   UseBiometrics: true :end
   PosIndex: 7 :end
   Assets: Area Available List :end
   AccessListLocal: Capt Lisko :end
   AccessListRemote: Capt Lisko :end
AccessListRemote: Lt LaMore :end
Network:
   Name: LAN 2 :end
   :end // of network description
ComponentProceduralSettings:
PasswordLength: Medium :end
PasswordCharacterSet: Moderate :end
PasswordChangeFrequency: six :end :end // ComponentProceduralSettings
:end // Component

Component:
   Name: Blato Desktop Select_11 :end
   IsTemplate: false :end
   AssetProtection: True :end
   HW: Blato Desktop Select :end
   Static: false :end
   Availability: 100 :end
   Resale: 200 :end
   OS: Populos V9 Desktop :end
   Software: POP.Mumo Virus :end
   User: TSgt Samuels :end
   PosIndex: 4 :end
   AccessListLocal: TSgt Samuels :end
   AccessListRemote: TSgt Samuels :end
   Network:
      Name: LAN 2 :end
      :end // of network description
ComponentProceduralSettings:
PasswordLength: Medium :end
PasswordCharacterSet: Moderate :end
PasswordChangeFrequency: six :end :end // ComponentProceduralSettings
:end // Component

Component:
   Name: Blato Desktop Select_12 :end
   IsTemplate: false :end
   AssetProtection: True :end
   HW: Blato Desktop Select :end
   Static: false :end
   Availability: 100 :end
   Resale: 200 :end
   OS: Populos V9 Desktop :end
   Software: Defiler :end
   Software: POP.Mumo Virus :end
   Software: POP.Sling Virus :end
   User: Lt LaMore :end
   PosIndex: 3 :end
   Assets: Air Tasking Order :end
   AccessListLocal: Lt LaMore :end
   AccessListRemote: Lt LaMore :end
   AccessListRemote: TSgt Samuels :end
   Network:
      Name: LAN 2 :end
      :end // of network description
ComponentProceduralSettings:
PasswordLength: Medium :end
PasswordCharacterSet: Moderate :end
Component:
  Name: Blato Desktop Select_13 :end
  IsTemplate: false :end
  AssetProtection: True :end
  HW: Blato Desktop Select :end
  Static: false :end
  Availability: 100 :end
  Resale: 200 :end
  OS: Populos V9 Desktop :end
  Software: POP.Mumo Virus :end
  User: TSgt Johnson :end
  PosIndex: 2 :end
  AssetProtection: Logistics Resource List :end
  AccessListLocal: TSgt Johnson :end
  AccessListRemote: TSgt Johnson :end
  AccessListRemote: Lt LaMore :end
  Network:
    Name: LAN 2 :end
      AccessList: *.Public :end
      AccessMode: YYYY :end
  :end // of network description
  ComponentProceduralSettings:
    PasswordLength: Medium :end
    PasswordCharacterSet: Moderate :end
  :end // ComponentProceduralSettings
  :end // Component

Component:
  Name: TS Encryptor Offsite :end
  IsTemplate: false :end
  Resale: 600 :end
  AssetProtection: True :end
  HW: Enigma2000 :end
  Static: false :end
  PosIndex: 9 :end
  Network:
    Name: TS :end
  :end // of network description
  AttachDevice: Enigma2000_5 :end
  :end // Device

Component:
  Name: S Encryptor Offsite :end
  IsTemplate: false :end
  Resale: 600 :end
  AssetProtection: True :end
  HW: Enigma2000 :end
  Static: false :end
  PosIndex: 10 :end
  Network:
    Name: S :end
  :end // of network description
  AttachDevice: Enigma2000_6 :end
  :end // Device

Component:
  Name: Enigma2000_5 :end
  IsTemplate: false :end
Resale: 250 :end
AssetProtection: True :end
HW: Enigma2000 :end
Static: false :end
PosIndex: 8 :end
Network:
    Name: LAN 1 :end
:end // of network description
AttachDevice: TS Encryptor Offsite :end
:end // Device

Component:
    Name: Enigma2000_6 :end
IsTemplate: false :end
Resale: 250 :end
AssetProtection: True :end
HW: Enigma2000 :end
Static: false :end
PosIndex: 3 :end
Network:
    Name: LAN 2 :end
:end // of network description
AttachDevice: S Encryptor Offsite :end
:end // Device

OPTIONS:
    UseScenarioCatalogItems: No :end :end

Briefing:
:end // Briefing

Conditions:

Condition:
    Tagname: MonthLong :end
    Parameter: 720 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    ConditionClass: TimeCondition :end :end

Condition:
    Tagname: OneDay :end
    Parameter: 9999 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    ConditionClass: TimeCondition :end :end

Condition:
    Tagname: FiveDays :end
    Parameter: 9999 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    Parameter: -1 :end
    ConditionClass: TimeCondition :end :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: TimeCondition :end
:end

Condition:
   Tagname: ThreeDays :end
Parameter: 9999 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: TimeCondition :end
:end

Condition:
   Tagname: TwoDays :end
Parameter: 9999 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: TimeCondition :end
:end

Condition:
   Tagname: Bankrupt :end
Parameter: 0 :end
Parameter: 1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: MinCashOnHand :end
:end

Condition:
   Tagname: MillerLackofProduct :end
   ConditionText: TSgt Miller :end
Parameter: 0 :end
Parameter: 40 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: UserProductivity :end
:end

Condition:
   Tagname: JohnsonLackofProduct :end
   ConditionText: TSgt Johnson :end
Parameter: 0 :end
Parameter: 40 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: UserProductivity :end
:end
Condition:
  Tagname: LiskoLackofProduct :end
  ConditionText: Capt Lisko :end
  Parameter: 0 :end
  Parameter: 40 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  ConditionClass: UserProductivity :end
  :end

Condition:
  Tagname: IntelPlansGoalFailure :end
  ConditionText: Maj Afinidad :end
  SecondConditionText: Access Intel Feed :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  ConditionClass: UserFailsGoal :end
  :end

Condition:
  Tagname: LogPlansGoalFailure :end
  ConditionText: TSgt Johnson :end
  SecondConditionText: Access Logistics Feed :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  ConditionClass: UserFailsGoal :end
  :end

Condition:
  Tagname: TSHack :end
  ConditionText: Intel Feed :end
  Parameter: 2 :end
  Parameter: 600 :end
  Parameter: 900 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  ConditionClass: AssetAttacked :end
  :end

Condition:
  Tagname: TSHackInternal :end
  ConditionText: Intel Feed :end
  Parameter: 1 :end
  Parameter: 10 :end
  Parameter: 900 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  ConditionClass: AssetAttacked :end
  :end

162
Condition:
Tagname: MostestMoney :end
Parameter: 10000 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
ConditionClass: MaxCashOnHand :end :end

/Of Conditions
Triggers:
Trigger:
TriggerName: GameLostCash :end
TriggerText: You are not that well funded
(PARAGRAPH)
FixedDelay: 0.000000 :end
RandomDelay: 0.000000 :end
FrequencyInDays: 0.500000 :end
ConditionList: Bankrupt :end
TriggerClass: LoseTrigger :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end

Trigger:
TriggerName: IntelLostProduce :end
TriggerText: Intel Plans was not able to produce the Target List for at least a day, this is detrimental to the mission of the AOC :end
FixedDelay: 1.000000 :end
RandomDelay: 1.000000 :end
FrequencyInDays: 0.500000 :end
ConditionList: MillerLackofProduct :end
TriggerClass: LoseTrigger :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end

Trigger:
TriggerName: LogLostProduce :end
TriggerText: Logistics Plans was not able to produce the Logistics Resource List for at least 2 days, this is unacceptable and you have been transferred to an Alaskan Weather Station :end
FixedDelay: 2.000000 :end
RandomDelay: 1.000000 :end
FrequencyInDays: 0.500000 :end
ConditionList: JohnsonLackofProduct :end
TriggerClass: LoseTrigger :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end

Trigger:
  TriggerName: WxLostProduce :end
  TriggerText: Weather Plans was not able to produce the Area Available List for at least 3 days, this incompetence has cost lives and you have been removed from your position :end
  FixedDelay: 3.000000 :end
  RandomDelay: 1.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: LiskoLackofProduct :end
  TriggerClass: LoseTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end

Trigger:
  TriggerName: BudgetReallocation :end
  TriggerText: A portion of your budget has been reallocated to support the fight against Canada :end
  FixedDelay: 0.000000 :end
  RandomDelay: 15.000000 :end
  FrequencyInDays: 0.400000 :end
  ConditionList: ThreeDays :end
  TriggerClass: BudgetTrigger :end
  Parameter: -8000 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end

Trigger:
  TriggerName: FailedIntelGoal :end
  TriggerText: Maj Afinidad is not able to fulfill her asset goal, make sure she has the means to her goal :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: IntelPlansGoalFailure :end
  TriggerClass: MessageTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end

Trigger:
  TriggerName: FailedLogGoal :end
  TriggerText: TSgt Johnson is not able to fulfill his asset goal to read the logistics feed, make sure he has the means to his goal :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.900000 :end
  ConditionList: LogPlansGoalFailure :end
  TriggerClass: MessageTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end

164
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
:end

Trigger:
  TriggerName: LosebyAttackSuccess :end
  TriggerText: The Intel Feed was compromised by an external attacker, you are an idiot. :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: TSHack :end
  TriggerClass: LoseTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
:end

Trigger:
  TriggerName: LosebyAttackSuccess2 :end
  TriggerText: The Intel Feed was compromised by an internal attacker, you are betrayed. :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: TSHackInternal :end
  TriggerClass: LoseTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
:end

Trigger:
  TriggerName: WinCashOverTime :end
  TriggerText: You have operated for 30 days, you have achieved victory :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 0.500000 :end
  ConditionList: MonthLong :end
  TriggerClass: WinTrigger :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
  Parameter: -1 :end
:end

Trigger:
  TriggerName: ATOPublished :end
  TriggerText: The ATO has been published :end
  FixedDelay: 0.000000 :end
  RandomDelay: 0.000000 :end
  FrequencyInDays: 1.000000 :end
ConditionList: OneDay :end
TriggerClass: TickerTrigger :end
Parameter: 9999 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
Parameter: -1 :end
: end

: end //Of Triggers
: EndOfFile
LIST OF REFERENCES


http://www.johnsaunders.com/paper/securitysimulation.htm


http://www.mitre.org/work/tech_paper_01/tanner_security/tanner_security.pdf; Cognitive Science and Artificial Intelligence Center, the MITRE Corporation, pp. 1 to 3.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. George Bieber
   OSD
   Washington, D.C.

4. RADM Joseph Burns
   Fort George Meade, Maryland

5. Deborah Cooper
   DC Associates, LLC
   Roslyn, Virginia

6. CDR Daniel L. Currie
   PMW 161
   San Diego, California

7. LCDR James Downey
   NAVSEA
   Washington, D.C.

8. Richard Hale
   DISA
   Falls Church, Virginia

9. LCDR Scott D. Heller
   SPAWAR
   San Diego, California

10. Wiley Jones
    OSD
    Washington, D.C.

11. Russell Jones
    N641
    Arlington, Virginia
12. David Ladd  
Microsoft Corporation  
Redmond, Washington

13. Dr. Carl Landwehr  
National Science Foundation  
Arlington, Virginia

14. Steve LaFountain  
NSA  
Fort Meade, Maryland

15. Dr. Greg Larson  
IDA  
Alexandria, Virginia

16. Ray A. Letteer  
Head, Information Assurance, HQMC C4 Directorate  
Washington, D.C.

17. Penny Lehtola  
NSA  
Fort Meade, Maryland

18. Ernest Lucier  
Federal Aviation Administration  
Washington, D.C.

19. CAPT Sheila McCoy  
Headquarters U.S. Navy  
Arlington, Virginia

20. Dr. Ernest McDuffie  
National Science Foundation  
Arlington, Virginia

21. Dr. Vic Maconachy  
NSA  
Fort Meade, Maryland

22. Doug Maughan  
Department of Homeland Security  
Washington, D.C.
23. Dr. John Monastra  
   Aerospace Corporation  
   Chantilly, Virginia

24. John Mildner  
   SPAWAR  
   Charleston, South Carolina

25. Marshall Potter  
   Federal Aviation Administration  
   Washington, D.C.

26. Dr. Roger R. Schell  
   Aesec  
   Pacific Grove, California

27. Keith Schwalm  
   Good Harbor Consulting, LLC  
   Washington, D.C.

28. Dr. Ralph Wachter  
   ONR  
   Arlington, Virginia

29. David Wirth  
   N641  
   Arlington, Virginia

30. Daniel Wolf  
   NSA  
   Fort Meade, Maryland

31. CAPT Robert Zellmann  
   CNO Staff N614  
   Arlington, Virginia

32. Dr. Cynthia E. Irvine  
   Naval Postgraduate School  
   Monterey, California

33. Paul Clark  
   Naval Postgraduate School  
   Monterey, California
34. Mike Thompson  
Naval Postgraduate School  
Monterey, California

35. Marc Meyer  
Captain USAF  
Naval Postgraduate School  
Monterey, California