NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A BUSINESS CASE ANALYSIS (BCA) OF THE ONE BOX – ONE WIRE (OB1) JOINT COMBINED TECHNOLOGY DEMONSTRATION (JCTD)

by

Paul J. Slaybaugh Jr.

March 2009

Thesis Advisor:	Daniel A. Nussbaum
Second Reader:	Steve Iatrou

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE *Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE A Business Case Analysis of the One Box – One Wire (OB1) Joint Combined Technology Demonstration (JCTD)

5. FUNDING NUMBERS

6. AUTHOR(S) Paul J. Slaybaugh Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The One Box One Wire (OB1) Joint Combined Technology Demonstration (JCTD) is a United States Central Command (USCENTCOM) initiative that has been approved by congress for a FY 2009 rolling start. The primary goal of the JCTD Program is to demonstrate, operationally assess, and transition capability solutions and innovative concepts to address the joint, coalition and interagency operational gaps and shortfalls in meeting the needs of the warfighter. Since inception in 1995, the Advanced Concept Technology Demonstration (ACTD) Program, and now the Joint Capability Technology Demonstration (JCTD) Program, has deployed critically needed warfighting solutions to every major Combatant Command theater.

The OB1 JCTD is an initiative designed to transform the existing Department of Defense (DoD) air-gapped networks (NIPR, SIPR, etc.) to an environment that allows the user to access all networks from a single PC terminal while still preserving the separation and security of data flows.

This thesis will be a business case analysis of the cost of implementing and sustaining the OB1 JCTD as compared to the current DoD multi-network infrastructure. This thesis will address the question of whether converting the existing military network infrastructure into OB1 is financially feasible. This thesis will concentrate specifically on OB JCTD initiative.

SUBJECT TERMS Business Case Analysis, BCA, One Box One Wire, OB1, Joint Combined Technology Demonstration, JCTD, Advanced Concept Technology Demonstration, ACTD, Special Operation Forces Cross domain services Architecture and System Enhancements, SOFCASE, High Assurance Platform, HAP, Classification Stateless Trusted Environment, CSTE, Coalition Secure Management and Operations System, COSMOS, Advanced Concept Technology Demonstration, ACTD, Agile Coalition Environment, ACE, Department of Defense Intelligence Information Systems, DoDIIS, DTW, NetTop

15. NUMBER OF PAGES
77

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** UU

THIS PAGE INTENTIONALLY LEFT BLANK

A BUSINESS CASE ANALYSIS (BCA) OF THE ONE BOX – ONE WIRE (OB1) JOINT COMBINED TECHNOLOGY DEMONSTRATION (JCTD)

Paul J. Slaybaugh Jr.
Lieutenant Commander, United States Navy
B.S., University of North Florida, 1999

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2009

Author: Paul J. Slaybaugh Jr.

Approved by: Dr. Daniel A. Nussbaum
Thesis Advisor

Steve Iatrou
Second Reader

Dr. Daniel C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The One Box One Wire (OB1) Joint Combined Technology Demonstration (JCTD) is a United States Central Command (USCENTCOM) initiative that has been approved by congress for a FY 2009 rolling start. The primary goal of the JCTD Program is to demonstrate, operationally assess, and transition capability solutions and innovative concepts to address the joint, coalition and interagency operational gaps and shortfalls in meeting the needs of the warfighter. Since inception in 1995, the Advanced Concept Technology Demonstration (ACTD) Program, and now the Joint Capability Technology Demonstration (JCTD) Program, has deployed critically needed warfighting solutions to every major Combatant Command theater.

The OB1 JCTD is an initiative designed to transform the existing Department of Defense (DoD) air-gapped networks (NIPR, SIPR, etc.) to an environment that allows the user to access all networks from a single PC terminal while still preserving the separation and security of data flows.

This thesis will be a business case analysis of the cost of implementing and sustaining the OB1 JCTD as compared to the current DoD multi-network infrastructure. This thesis will address the question of whether converting the existing military network infrastructure into OB1 is financially feasible. This thesis will concentrate specifically on OB JCTD initiative.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The One Box One Wire (OB1) Joint Combined Technology Demonstration (JCTD) is a United States Central Command (USCENTCOM) initiative that has been approved by congress for a FY 2009 rolling start. The primary goal of the JCTD Program is to demonstrate, operationally assess, rapidly deploy, and transition capability solutions and innovative concepts to address the joint, coalition and interagency operational gaps and shortfalls. Since inception in 1995, the Advanced Concept Technology Demonstration (ACTD) Program, and now the Joint Capability Technology Demonstration (JCTD) Program, has deployed critically needed warfighting solutions to every major Combatant Command theater.

Rolling starts have been successfully vetted through the JCTD process however; there still remains a product development or resource management issue that needs to be resolved with the stakeholders prior to project initiation

The OB1 JCTD is an initiative designed to transform the existing Department of Defense (DoD) air-gapped networks (NIPR, SIPR, JWICS, CENTRIX) to an environment that allows the user to access all networks from a single PC terminal while still preserving the separation and security of data flows. The ineffectiveness of air-gapped networks results in dangerous challenges to successful multinational operations with increasing cost to life and high risk to mission failure.

This thesis will be a business case analysis of the cost of implementing and sustaining the OB1 JCTD as compared to the current DoD multi-network infrastructure. In order to meet that objective it will address the question of whether converting the existing military network (NIPR, SIPR, JWICS, MCFI, CENTRIX, etc.) infrastructure into OB1 is financially feasible. This thesis will concentrate specifically on OB JCTD initiative.

Specific research questions include: the cost of implementing OB1, to include, research and development (R&D) and procurement, the savings of OB1 verses current infrastructure, and in what infrastructure will OB1 be implemented.

The results of the OB1 business case analysis are as follows:

- OB1 has a NPV Savings of $263.1M
- OB1 has a ROI of 662.9%
- Positive savings and ROI are realized from the first year of OB1 implementation
- The base case annualized ROI never falls below 275.6% when the discount factor was varied from 3% to 10%
- The base case annualized ROI does not fall below 683.4%, even when the initial investment cost to field OB1 is increased by $20.0M
- The base case annualized ROI does not fall below 231.7%, even when varying the recurring investment costs from 0% to 1000%
- Given a worst-case scenario for OB1:
    - OB1 still yields a ROI of 49.9%
- The analysis conducted in this thesis shows that financially, OB1 is a viable and robust solution to the problem of having multiple air gapped networks. OB1 provides a high return on investment over a wide range of varying input factors and appears to be a worthwhile investment for the DoD.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my beautiful wife of nearly 20 years, Bridget, for her constant encouragement and support. Even though our Navy life hasn’t always been easy, and together, over the years, we have endured many hardships, she has always been fully supportive and understanding. Though I have not always been there for her, she has been there for me every step of the way, from moving to buying homes to having babies, all without me by her side. She has made me a better person, and I am who I am today all because of her. For that I will be forever grateful.

I would also like to give a heartfelt thanks to my thesis advisor, Dr. Dan Nussbaum. His mentorship, guidance and support throughout this experience have been second to none. I cannot imagine having a thesis advisor more approachable, down to earth or more available. Thank you for your time and thank you for making my thesis experience as enjoyable as possible.

Steve Iatrou’s due diligence in reviewing my thesis and guidance in helping me navigate the final stages of the thesis process were also much appreciated.

The entire OB1 team was extremely professional and supportive throughout this process. They are a first-class group from which I have learned a great deal. Jerry “Too Big” Gelling and Bud Jones at CENTCOM were of particular help throughout this process. They provided me with much of the data for this thesis, as well as their invaluable feedback, guidance and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE AND BACKGROUND OF THE STUDY

The One Box One Wire (OB1) Joint Combined Technology Demonstration (JCTD) was born at the United States Central Command (USCENTCOM) MacDill Air Force Base in Tampa, Florida. It was here that CENTCOM's Science and Technology Advisor discovered there was a problem. He observed that many desks were cluttered with multiple personal computers, monitors and miles of cabling. Not only that, even though CENTCOM buildings were relatively new, there was a tremendous amount of extra cooling capacity required to cool all this equipment. There was a call put out to the scientific community and the Multiple Independent Levels of Security (MILS) Group responded. Eventually, they went to CENTCOM and briefed them on MILS technology that was currently available. Some of these technologies were being used in the F-35 Joint Strike Fighter (JSF), the F-22 Raptor and the Joint Tactical Radio System (JTRS) programs. It is the embedded software in these programs that provide a separation kernel which allows multiple independent levels of security (TOP SECRET to UNCLASSIFIED) in the aircraft on-board computer. CENTCOM inquired if the software could be used in a Local Area Network (LAN) environment and in August 2007, two commercial vendors, Green Hills Software (GHS), and Objective Interface Solutions (OIS), responded with a proposal that would solve their problem. The primary components of which include the INTEGRITY® secure operating system and separation kernel by GHS, a Black Channel gigabit switch and a Black Channel network interface card (NIC) provided by OIS.

The OB1 JCTD is a USCENTCOM initiative that has been approved by congress for a FY 2009 rolling start. According to the FY 2009 JCTD (2008), the primary goal of the JCTD Program is to demonstrate, operationally assess, rapidly deploy, and transition capability solutions and innovative concepts to address the joint, coalition and interagency operational gaps and shortfalls. Since inception in 1995, the Advanced Concept Technology Demonstration (ACTD) Program, and now the Joint Capability Technology Demonstration (JCTD) Program, has deployed critically needed warfighting solutions to every major Combatant Command theater. Rolling starts have been successfully vetted through the JCTD process; however, there still remains a product development or resource management issue that needs to be resolved with the stakeholders prior to project initiation.

The FY 2009 JCTD Congressional Notification (2008) states:

> By design, the JCTD program is not an acquisition program, but it is intended to jump-start the acquisition process through successful, innovative demonstrations of mature technology…The JCTD program is integrated with the Joint Capability Integration and Development System (JCIDS) developed by the Joint Chiefs of Staff (JCS). The JCTD process seeks to increase upfront transition planning of the concepts and technologies demonstrated…The adaptive JCTD process provides an agile technology development and demonstration program to better address the threats of an enemy who is not hampered by a rigid and more deliberative budgeting and acquisition process. (p. ii)

Another major goal of the JCTD program is to have a demonstration of concept in two to four years and critical Combatant Commander (CoCom) capability in two to three years with a major focus on tactics, techniques and procedures (TTPs). Often referred to as the "80% solution" with a "try with intent to buy" philosophy the transition and acquisition strategy is not fully developed until significant military capability (via testing and operational demonstrations) has been verified by the CoComs. The JCTD process is also designed to streamline the acquisition process by incorporating spiral technology insertion and risk mitigation potential (FY 2009 JCTD, 2008, p. iii).

The purpose of this study is to analyze the cost savings and benefits of implementing the OB1 JCTD. Specifically, this research will:

- Describe other potential alternative technologies to OB1. This discussion will also include analysis as to why or why not these alternatives are viable options.
- Conduct an OB1 JCTD business case analysis, including a baseline analysis and an extensive sensitivity analysis.

B. PROBLEM STATEMENTS

There are several operational policies and constraints in place today that inhibit information sharing and collaboration universally amongst joint, coalition and inter-agency warfighters. According to the OB1 team some of those limitations are (Network, 2008, p. 2):

- Inability to rapidly share, collaborate on, or synchronize operational or intelligence information between mission partners
- Degraded capability to provide an assured environment to rapidly access relevant, accurate, and timely information
- Limited capability to interoperate with and leverage mission partner systems
- Inability to extend U.S. capabilities to mission partners rapidly and within a net-centric environment
- Limited resources to operate, maintain, and defend the multiple separate physical infrastructure/networks required by current policy
- An inability to create a single environment that enables the sharing of information at tactical through theater levels and within multiple classification domains
- Limited access to a coalition networks require creating information on the SIPRNET and transferring files via an air gap[1] technique

In their draft CONOPS the OB1 team states, “These limitations and constraints result in U. S. forces having no cohesive, integrated, effective, efficient, or flexible means to seamlessly and quickly share critical information with mission partners. This ineffectiveness results in dangerous challenges to successful multinational operations with increasing cost to life and high risk to mission failure” (Network, 2008, p. 2).

[1] An air gap is a security measure often taken for computers and computer networks that have extreme security requirements. The architecture must ensure that secure networks are completely physically, electrically, and electromagnetically isolated from insecure networks, such as the public Internet or an insecure local area network.

C. CASE FOR CHANGE

1. Technical Environment

Like most of today’s military forces across DoD and across the world USCENTCOM has the need for multiple networks in order to accomplish its mission. At CENTCOM, SIPRNET (SECRET network) and NIPRNET (UNCLASSIFIED network) are extremely prolific and present on almost every users’ desk. CENTCOM, as well as most other Combatant Commands, have a need for coalition networks. Other coalition networks include the CENTRIXS Multinational Coalition Forces Iraq (MCFI), CENTRIX Global Counter Terrorism Forces (GCTF) and bilateral networks.

The large footprint required for the current DoD network architecture puts a huge economic, financial and logistics burden on combatant commanders and ultimately the warfighter. The requirement to have these networks air gapped and the inability to collapse them into a smaller footprint significantly increases the expense of the network, the infrastructure itself and the time to install and maintain.

2. Operational Environment

Today’s enemy is elusive and resourceful. The enemy that our military faces today is looking less and less like the traditional enemy of old. Instead of our military engaging in campaigns against well defined nation states with known armies, our military is increasingly fighting an enemy that has no state boundaries, no readily apparent army and does not fight by traditional rules of war. Our new enemy is increasingly radical, elusive and operates without concern for traditional nation borders. It is an enemy that can rapidly adapt and maneuver; it is very adept at not only mobilizing its own forces, but those of the local population, and indeed, the global community, as a whole. This enemy is increasingly able to employ technology at his disposal in a way that can quickly and effectively shapes global perceptions in his favor.

Our enemy is increasingly winning the Information Operations (IO) battle. COL Ralph O. Baker, former Commanding Officer of the 2d Brigade Combat Team of the 1st Armored Division in Baghdad, expressed his frustration with his superior’s inability to get his units version of events out to the media before the enemy in an article he wrote for

Military Times in May 2006. According to COL Baker (2006), “While precious time was being spent ‘gathering facts’, the enemy was busily exploiting to their advantage the ensuing chaos. The message they passed to the press was that…the carnage on the street was not the result of a VBIED but, rather, the result of an undisciplined and excessive use of force by my Soldiers” (p. 17). In today’s world information is readily abundant and, perception is reality. In order to build a strong coalition and garner the support of the local population in theater, the U.S. military needs to get its version of events to the media before the enemy.

Therefore, it is CENTCOM’s belief and guidance[2] that their information sharing capability must move forward in a way that gives warfighters the ability to shape the IO battlefield in CENTCOM’s favor. CENTCOM claims OB1 will help achieve this by providing timelier, accurate information that the warfighter and his commander can use to, not only shape the physical battlefield, but the IO battlefield as well.

“The future joint force requires an agile information sharing environment supporting tactical, operational, and strategic military operations and training with mission partners” (Network, 2008, p. 2). According to CENTCOM, “…the current architectural footprint is something they can no longer continue to scale operationally, logistically or financially.”

The CENTCOM team argues in their CONOPS (Network, 2008):

> The United States will probably always fight as a joint/coalition force in the future. The political nature of Coalition compositions depends on the mission and situation, and sometimes requires us to operate under bilateral agreements. Our current security policy requires that the network classification domains must be kept separate, hence multiple physical networks. This model has resulted in the deployment of multiple sets of computing infrastructure—a solution that we cannot continue to scale operationally, logistically, or financially. (p. 4)

[2] Noted in USCENCOM’s Requirements Statement for Network Infrastructure Consolidation dated October 2007.

D. RESEARCH METHODOLOGIES, LIMITATIONS AND ASSUMPTIONS

To achieve the purpose outlined in section I.A., we researched various online websites and corresponded with several program managers and team members of the various alternatives to OB1 in order to gain background information and an operational description of those technologies. Next, a literature review was conducted on business case writing and recommended analytic structure. My thesis advisor and I have conducted a critical financial analysis of data obtained from CENTCOM during their initial analysis of the financial viability of OB1. Finally, this thesis reports the results of the OB1 JCTD business case analysis and makes relevant recommendations for decision makers.

The following assumptions were made during the conduct of this analysis:

- The cost savings derived from the business case analysis based on the data available from a service or system can be applied across services and systems.
- A conservative approach is adopted for the business case analysis. That is, when there is a choice between higher and lower costs, the higher cost will be used for the analysis. Similarly, when there is a choice between higher and lower benefits, the lower benefit will be used for the analysis.

II. ANALYSIS OF ALTERNATIVES (AOA)

There are several other technologies, either fully or partially developed, that CENTCOM has evaluated as possible alternatives to OB1. From Table 1 we can see each alternative to OB1 that CENTCOM has evaluated and reasons each technology does not meet CENTCOM requirements. Check marks indicate failure to meet a particular requirement.

	High Robustness	Evaluation Artifacts	CENTCOM IA Req'ts[3]	Collapse Networks	Collapse Workstations	Cost Effective
SOFCASE	✓	✓	✓			
HAP	✓	✓		✓		
CSTE	✓	✓				
COSMOS	✓			✓	✓	
ACE	✓	✓		✓		
DTW	✓			✓		✓
NetTop	✓	✓				
OB1						

Table 1. Alternative technologies to OB1 and CENTCOM requirements

A brief synopsis of each CENTCOM reviewed AoA, as well as, reasons they do not achieve the OB1 objectives, follows:

[3] CENTCOM uses chapter four of the Information Assurance Technical Framework to determine their assurance levels.

A. SPECIAL OPERATION FORCES CROSS DOMAIN SERVICES ARCHITECTURE AND SYSTEM ENHANCEMENTS (SOFCASE)

SOFCASE is a project that is leveraging two major government efforts; the High Assurance Platform (HAP) (managed by the National Security Agency (NSA)) and a Cross Domain Solution (CDS) called Information Support Server Environment (ISSE) managed by the Air Force Research Lab (AFRL). The United States Southern Command (USSOCOM) is building an architecture to address some specific technical, operational and acquisition requirements that are using technologies out of existing programs within these two organizations.

SOFCASE is not a viable alternative to OB1 because there is no current plan to meet high robustness, develop evaluation artifacts or meet CENTCOM assurance requirements for threat levels (Staneszewski, 2008, p. 39).

B. HIGH ASSURANCE PLATFORM (HAP)

According to the National Security Agency (NSA) website (High, 2009), "HAP is a multi-year NSA program with the vision to define a framework for the development of the next generation of secure computing platforms. NSA conducts this effort in collaboration with industry, academia, and other government organizations."

The secure computing workstations the HAP program intends to build use commercial-off-the-shelf (COTS) security technologies coupled with the latest information assurance (IA) techniques. This allows commercial vendors to develop assurable secure, manageable, and usable computing platform component products that integrate with a common architecture that will enable integrators to deliver COTS-based assurable commercial solutions to DoD, government and commercial entities (High, 2009).

HAP objectives include:

- Provide a secure computing platform execution environment for operational users
- Enable technology integrators to compose cost-effective assurable platform instances from COTS components

- Enable COTS technology developers to build assurable platform components (hardware, software, firmware, I/O devices etc.)

Even though HAP is pursuing a one wire solution similar to OB1 the time frame on that is approximately FY 2014. That timeframe together with the fact they have no current plans for High Robustness makes HAP a less than desirable alternative to OB1. (Staneszewski, 2008, p. 39).

C. CLASSIFICATION – STATELESS, TRUSTED ENVIRONMENT (CSTE) JOINT COMBINED TECHNOLOGY DEMONSTRATION (JCTD)

CSTE is a Special Operations Command (SOCOM) sponsored JCTD. According to SOCOM, CSTE is "An assured (trusted) electronic environment that has no inherent classification state when not processing or displaying data and is independent of the classification level of the network(s) to which it is attached." Its primary objectives are to have an ability to rapidly and securely share both unclassified and classified information between multiple coalition partners on a common operating system (network). As well as have a network that has the ability to quickly and dynamically host new capabilities and users.

In order to meet these objectives, CSTE incorporates a data object encapsulation component. These data objects are encrypted and can be in only one of four states: at rest, in transit, in process or being displayed. The Data Object Protection System (DOPS) enables the protection of information based on its content at the point of origin. CSTE with DOPS implementation has several advantages:

- It implements encryption of information (data at rest) on the local device
- Access is based on content of the information, user's authorizations and location, and the capability of the device
- It decouples the need for the infrastructure to protect the data

Encryption of the data object is critical for creating a classification–stateless environment and will protect the data when CSTE is under attack.

According to the OB1 team, CSTE does not meet their objectives because there is no current plan to meet High Robustness or develop evaluation artifacts (Staneszewski, 2008, p. 39).

D. COALITION SECURE MANAGEMENT AND OPERATIONS SYSTEM (COSMOS) ADVANCED CONCEPT TECHNOLOGY DEMONSTRATION (ACTD)

COSMOS is a European Command (EUCOM) and Pacific Command (PACOM) sponsored ACTD. In addition to the U.S. the ACTD involves Australia, Canada, Great Britain and more recently, Singapore. The goal is rapid, secure release and protection of critical command and control (C2) information to and among coalition partners on a single and secure integrated coalition network to reduce confusion, uncertainty and delay in combat and crisis operations. The net result will be the bridging of coalition sourced information with U.S. Global Information Grid (GIG) Network Centric Enterprise Services (NCES) for two-way information exchange.

The history of COSMOS stems from Operation Iraqi Freedom (OIF) when Marine Forces Central Command (MARFORCENT) could not rely on sneaker-net[4] information because all of the restrictions and security measures in place impeded operations and led to confusion. Today, COSMOS participants are developing a way to allow the unambiguous sharing of information between coalition partners and attempting to collapse the number of operational networks required, while maintaining need-to-know levels of separation. COSMOS will also implement the Multilateral Interoperability Program (MIP) C2 Information Exchange data Model (C2IEDM) and Data Exchange Mechanism (DEM) to address the unambiguous sharing aspects and use VPN technology augmented with configuration and control tools to achieve the need-to-know separation requirements. The United States National Security Agency (NSA) is overseeing the design of the security components. Each participant nation will validate this approach against a national C2 system.

[4] The transfer of electronic information, especially computer files, by physically carrying removable media such as magnetic tape, floppy disks, compact discs, USB flash drives, or external hard drives from one computer to another.

A brief by the COSMOS team ("COSMOS Aims", 2009) states:

> There is more to multinational unity of effort than sharing C2 information, but the better the sharing, the better the potential for good multinational unity of effort. COSMOS improves C2 information sharing by adding automation, security and dynamic management. Multinational partners are interested in sharing C2 information and commanders and coalitions have specific situation and role-based needs. However, each nation has long-term interests that can undercut short-term unity of effort. (p. 4)

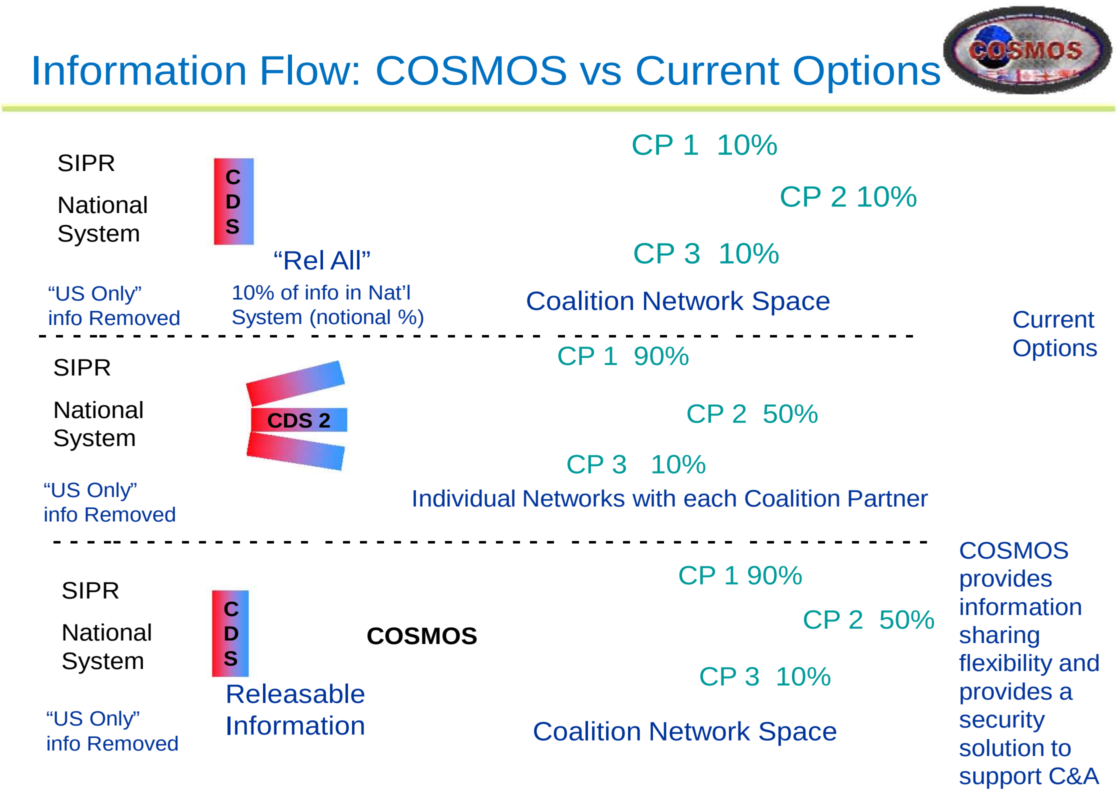


Figure 1. COSMOS vs. Current Operations [From Cosmos Aims, Fig 1-1]

The top line of Figure 1 shows the current network architecture for the SIPRNET across DoD. In this scenario there is a release of information via a CDS to a multinational "space" or network cloud. Within this cloud all information is shared with all partners. The problem with this infrastructure is that based on the current operational and/or tactical scenario more applicable information can and should be released. However, long-term multinational interests significantly reduce this flow.

The middle row represents a current architecture that is sometimes employed, i.e., having many separate networks. Problems with this approach include: high overhead in terms of equipment for the physical network, and it does not give a commander the ability to adjust what information is disseminated as the operation and battle space evolve.

The bottom option is what COSMOS claims it can do for the customer. This is also the preferred architecture suggested the by GIG IA strategy. This type of network environment puts a U.S. node or enclave in the national space with sufficient information security tools and information management tools that the commander can stage the C2 information he might share with partners (just as he stages ammunition and fuel forward) in the enclave and then share information with partners as appropriate for the changing circumstances of the battlefield.

It takes many months to build, test, and certify the rules for a CDS for a specific operation in a specific theater. One of the greatest advantages of COSMOS is that it allows real-time changes to information exchanges with coalition partners.

Even with these advantages, the COSMOS ACTD does not meet the objectives of OB1 because it does not collapse workstations or networks with multiple security levels. Also, COSMOS is data-centric and does not provide a network solution (Staneszewski, 2008, p. 39).

E. AGILE COALITION ENVIRONMENT (ACE)

The ACE architecture will soon be installed as component of the Commander Third Fleet (C3F) command and control (C2) Network. Physical location for the installation is C3F Headquarters in San Diego, CA, the Pacific Regional Network Operations Center (PRNOC) and Naval Communications and Telecommunications Area Master Station Pacific (NCTAMSPAC) on the island of Oahu in Hawaii.

“The Agile Coalition Environment (ACE) system is a combination of commercial off-the-shelf (COTS) and open source products designed to provide users with the ability to access multiple U.S. and allied/Coalition secure domains from a single workstation” (Referentia Systems Inc., 2007, p. 5).

The ACE program consists of a combined synergistic group of emerging network-centric and information assurance (IA) technologies. These combined ACE technologies provide the warfighter with enhanced information sharing, collaborative tools, and situational awareness capabilities that are both dynamic and secure. Warfighters have access to all required user applications and multiple security enclaves of information at a single workstation. Interoperability is achieved across all applications, platforms, and security domains. ACE is presented as a network capability that can be applied to the Combined Enterprise Regional Information Exchange System (CENTRIXS) as well as other coalition or Community of Interest (COI) networks that require information sharing across multiple security domains between U.S. and coalition forces. ACE technologies have evolved during a four-year spiral development cycle and have targeted warfighters at all levels for improving interoperability and knowledge management for current and future joint and coalition operations. This evolution for developing tomorrow's IT capabilities has been based on requirements, technology insertion, operational experimentation, and improvements as a result of Joint, Coalition, and Naval Fleet feedback (Referentia Systems Inc., 2007, p. 5).

According to Referentia Systems Inc (2007):

> The ACE architecture is designed to provide access to multiple security enclaves from a single terminal through the use of two Cross Domain Management Office base lined capabilities: NetTop 1.3.1 and JANUS 5.1. NetTop uses Virtual Machines (VMs) to provide separation on the client terminal between security enclaves. A terminal user is not allowed to move information between enclaves. The C3F installation will consist of 14 ACE terminals that will be capable of accessing SIPRNET, Combined Enterprise Regional Information Exchange System – 4Eyes (CENTRIXS-4Eyes), the Cooperative Maritime Forces Pacific (CMFP) virtual private network (VPN) on Combined Enterprise Regional Information Exchange System – Global Counterterrorism Force (CENTRIXS-GCTF) , and Combined Enterprise Regional Information Exchange System – Japan (CENTRIXS-JPN). (p. 5)

For the C3F setup in San Diego and Hawaii, the ACE terminal uses NetTop 1.3.1 to create “Fat” and “Thin” Virtual Machines (VMs) (referred to as “GUI” VMs) that connect to the four security domains. For SIPRNET, the ACE Terminals will use a Fat VM that will allow the use of any data type that the SIPRNET applications use. For the three CENTRIXS networks, the ACE Terminals will use a Thin VM. For the Thin VMs only, ICA type traffic will be used to communicate with Citrix servers located in the respective CENTRIXS data centers (Referentia Systems Inc., 2007, p. 5).

ACE achieves security separation through the use of NetTop, VMs and Virtual Private Networks (VPNs). Each VM is tied to one VPN VM that uses and IPSec client to establish a connection with a VPN Concentrator in the data center. All ACE terminals and associated VMs are capable using one network interface card (NIC). Note in Figure 2 that the ACE terminals have no interaction with VPN VM. VPN VMs are automatically launched when the graphical user interface (GUI) VM is launched and they stay open until the GUI VM is shut down (Referentia Systems Inc., 2007, p. 6).

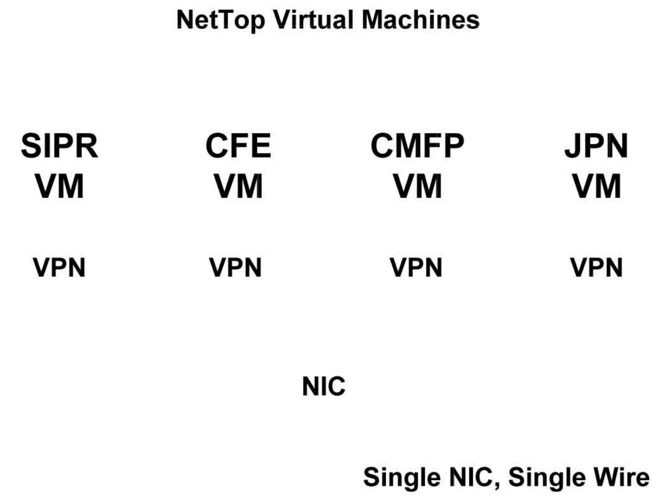


Figure 2. NetTop VMs in an ACE architecture [From Referentia Systems Inc, Figure 1]

Some of these concerns may not be valid, the OB1 team claims that the ACE technology does not collapse multiple networks, does not support High Robustness and there are no current plans to generate evaluation artifacts (Staneszewski, 2008, p. 39).

F. DEPARTMENT OF DEFENSE INTELLIGENCE INFORMATION SYSTEMS (DODIIS) TRUSTED WORKSTATION (DTW)

DTW was designed for and is mostly used by the DoD intelligence community. "DTW is an Air Force Command, Control, Intelligence, Surveillance, and Reconnaissance Center sponsored, Defense Intelligence Agency (DIA) directed capability for using a single desktop workstation to access all DoDIIS data and applications available to a particular user from multiple, concurrent security domains" (DoD Trusted, 2006). It is designed to provide a standard intelligence system coupled with applications interoperability that enables collaboration between intelligence sites in a secure and timely manner. DTW is an initiative that was jointly developed by Sun Microsystems and Trusted Computer Solutions (TCS).

1. DTW and Trusted Computer Solutions (TCS)

The TCS website states:

> As with all organizations managing critical intelligence tasks, DoD intelligence sites face a major challenge in securely sharing information in a timely manner. This challenge led the Defense Intelligence Agency (DIA) to turn to a commercial-off-the-shelf (COTS) product from Trusted Computer Solutions (TCS), a leader in secure information sharing. They selected the TCS flagship desktop product, SecureOffice® Trusted Workstation™, as an integral component of the Department of Defense Intelligence Information Systems (DoDIIS) Trusted Workstation (DTW). The DIA then assigned the Joint Enterprise DoDIIS Infrastructure (JEDI) Program Management Office (PMO) to manage the program. The use of a single, ultra-thin client via Trusted Workstation to access multiple levels of classified data and then disseminate actionable information provides many benefits, including: enhanced security, enhanced functionality, enhanced audit management, simplified installation and administration, reduced support costs and ease of certification and accreditation. DTW enables intelligence organizations to ensure high-risk processes are automated in a predictable, auditable and accreditable manner. (JEDI PMO, n.d.)

2. DoDIIS Trusted Workstation

DoDIIS Trusted Workstation is a JEDI PMO managed standard solution that includes the following features (JEDI PMO, n.d.):

- Ultra-Thin Client Appliance
- Full Microsoft® Windows® application and network functionality
- E-mail, Web browsing and collaboration
- JEDI Tools – Trusted Session Maintenance, Trusted User Maintenance, Enhanced Password Rules, User Password Utility, and Jumpstart scripts
- TCS Trusted Relabeler – enables the secure movement of information between security levels
- TCS trusted administration and configuration tools
- Existing application integration
- Simultaneous access to multiple classified networks
- Single DTW baseline image

3. DTW Return-on-Investment

Because DTW helps individuals, and therefore organizations, gain access to secure information across multiple networks and classification levels using familiar software applications DTW enables organizations to improve security and accountability in the high op-tempo environment that today's DoD operates in. Other advantages include (JEDI PMO, n.d.):

- Dramatically decrease the number of desktop workstations via ultra thin client architecture
- Reduce network and infrastructure costs
- Increase intelligence staff productivity
- Reduce information technology staff workload
- Provide simultaneous access to multiple networks across classification levels from a single screen
- Provide session mobility
- Previously accredited and operational solution

However, as the OB1 team (Staneszewski, 2008, p. 39) points out, and verified in a separate report by NYTOR Technologies (The DoDIIS, 2007, p. 3), one of the major disadvantages to DTW is that DTW is accredited under Director of Central Intelligence Directive (DCID) 6/3 (manual for protecting sensitive compartmented information (SCI) within information systems) at a level that only permits access to networks ranging from SECRET (including collateral) through TS/SCI simultaneously. Also, according to the same reports from OB1 and NYTOR, DTW cost up to ten times what OB1 would (cost per seat: $10k-$18k). Furthermore, it does not provide high robustness (Staneszewski, 2008, p. 39) or provide access to UNLCAS networks (The DoDIIS, 2007, p. 3).

Other possible concerns with DTW addressed in the May 2007 white paper by NYTOR technologies (The DoDIIS, 2007) include:

- All program execution occurs on the server; applications that cannot be executed in a Citrix shared application environment are not supported
- Streaming video executes on the server, resulting in exceptionally high bandwidth requirements and poor performance
- Smartcard does not provide strong authentication or use an X.509 certificate
- Does not provide machine authentication
- Does not support printing
- Does not provide USB support
- Does not provide expansion slots
- Does not presently support multiple monitors
- Requires Trusted Solaris administrators to maintain its server-side infrastructure
- Is better suited for environments where there is a strong need for UNIX applications or UNIX is already the dominant operating system

G. NETTOP

NetTop was initially developed in 1999 by the National Security Agency (NSA). It was about this time the NSA realized much of its technology was changing over from government produced products to commercial products. It was with this transition, combined with the rapid growth of information technologies and the even more rapid increases in cheaper and faster computing power, that the NSA realized it could not keep pace in its ability to protect information processed by the national security community. Historically, technologies flowed from within government to our homes. The Information Age and explosion in cost effective computing power has begun to reverse that trend. Now more and more technologies are coming from commercial vendors vice inside government and NSA. To further exacerbate the information assurance problem NSA also realized more and more R&D dollars were going away from areas designed to protect the data to that of intrusion detection and response (NetTop Commercial, 2000, p. 1).

To address the issues the NSA Advisory Board (NSAAB) challenged the Information Assurance Research Office (IARO) to develop architectures that would not only have the look and feel of Commercial-off-the-shelf (COTS) products but would utilize them as well. Key to the success of the team would be the ability to use the new technology in a high assurance environment. The result of their effort is NetTop (NetTop Commercial, 2000, p. 1).

As is the case with OB1, and the rest of these alternatives, NetTop attempts to address one of the major concerns for the warfighter and that is the amount of desktops (CPUs, monitors, keyboards, mice, etc.) that are necessary in order to have access to multiple networks of different sensitivity at one user workstation. Other concerns NetTop attempts to address are: previous government based security solutions have been incompatible with other standards based IT products, this complicates the interoperability and upgrading of components, cost and complexity of network administration and the ability to rapidly add and remove users holding multiple security levels and from multiple DoD, government agencies and multiple coalition partners. In general the overarching goal of NetTop (as well as, OB1 and most of the other alternatives) is to deliver multiple network domains to one workstation in order to eliminate redundant hardware and reduce the total cost of ownership (TCO) of high-assurance computing.

One of the consequences of requiring a high assurance platform for the end-user is that the end-user's environment must be considered untrustworthy. NetTop architecture must protect against potentially hostile behavior. In order to do this, NSA began to explore the concept of encapsulation to limit, or minimize, the effects of the end-user OS and application software.

According to Meushaw and Simard (2000):

> The method selected for encapsulating the OS was based upon a 30-year-old technology, Virtual Machine Monitors (VMM). VMM technology was designed and developed in the era of large IBM mainframe computers, and was intended to help extend the life of legacy software, when improved hardware or OS software was released. In essence, a VMM was a software system that ran directly on the computer hardware, and allowed multiple operating systems to be installed on top of it. By running older OS versions in some virtual machines, legacy software could be run, while newer application software could be executed in virtual machines (VM) running more current OS versions. During this initial design and production phase NSA discovered a new commercial product called VMware. VMware provided a commercially available application that could be integrated with VMMs. The VMware product is a spin-off of DARPA-sponsored research at Stanford University, and is generally used for providing a safe test environment for OS and networking software. (p. 2)

Meushaw and Simard (2000, p.2) also claimed VMware had several advantages that made it attractive to the NetTop design team:

- VMware was designed for efficient operation on Intel x86 platforms vice large mainframe computers. This made it more suitable for NetTop's end-user who uses laptops, PCs and Thin Clients
- VMware operates on top of an underlying host OS rather than directly on the system hardware
- VMware provides and abstraction for virtual Ethernet hubs. Allows virtual machines to be interconnected in a way that is well understood by network administrators and designers

In 2005 NSA reached a licensing agreement with two commercial vendors which allows them to develop and market NetTop technology. Those commercial vendors are Hewlett Packard (HP) and Trusted Computing Solutions (TCS). Both vendors are using the SELinux OS as the main building block in their architecture. Even though both vendors benefit from all the advantages of NetTop technology, there are subtle differences in the technology used by the vendors, which meet the original final objectives of the NSAAB. Both HP and TCS systems are currently undergoing certification and accreditation.

1. HP NetTop

A HP technical report (“HP NetTop”, 2004) posted on their website describes their version of NetTop as follows:

> Between the VM vaults provided by SELinux policy and the absence of any communication interface in the HP NetTop SELinux host OS, HP NetTop can be viewed as a software keyboard, video, mouse (KVM) device for switching between VMs. You don’t need separate networks and multi-network interface card (NIC) workstations to benefit from HP NetTop. HP NetTop works with VPNs to provide end-to-end data encryption between different VMs and their virtual private network (VPN) termination points. In the same way that VMs can be bound to different physical NICs connected to different network backbones, this single network solution allows HP NetTop to be used in any network where secure data separation is required. (p.3)

An operational description of NP NetTop is shown in Figure 3.

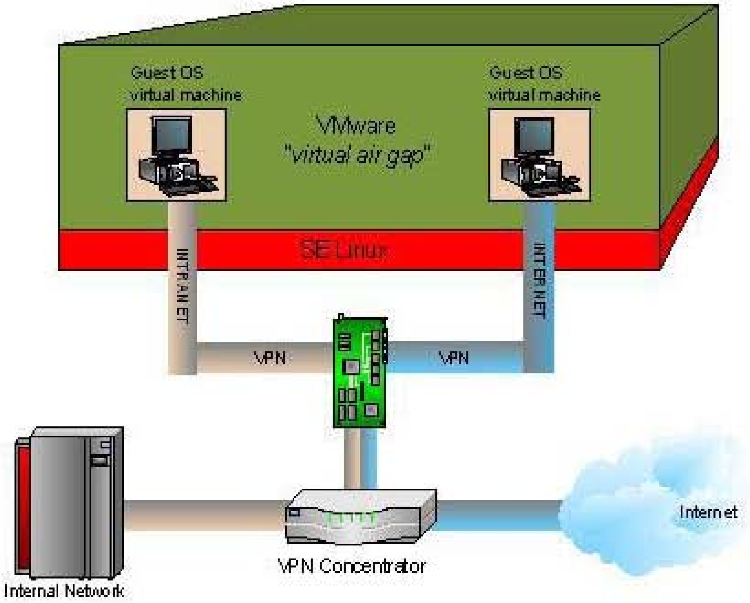


Figure 3. HP NetTop [From HP NetTop, Fig 2]

2. TCS NetTop

TCS NetTop also uses SELinux as for the host OS. However, a major difference between the HP architecture and TCS is that TCS does not use VPN technology as its core piece of equipment used to link multiple networks. TCS has developed what it calls a Distribution Center (DC). It is this DC that controls all networking and routing functions. The DC is also a SELinux based system that provides a multilevel gateway to single level networks (a properly configured NIC is required for each system high network). The DC handles the administrative functions via a user friendly graphical user interface (GUI), automatically commonly configures and authenticates each end-users Thin Client (workstation) and provides automatic failover and load distribution (SELinux Symposium, 2007, p.10).

OB1, and many of these alternatives to OB1, have the ability to set up their network with Thin Clients on the user end. The use of Thin Clients for the end user has many advantages, most notably, in the area of information assurance and computer security. TCS has done an excellent job of leveraging all the advantages of Thin Client computing and the NSA approved NetTop technology.

However, according to the OB1 team, NetTop alone does not meet the OB1 objectives of High Robustness and development of evaluation artifacts (Staneszewski, 2008, p. 39).

As you can see from Table 1 in the beginning of this chapter, these alternatives to OB1 meet some, but not all, of the criteria set forth by the CENTCOM commander in his Requirements Statement for Network Infrastructure Consolidation ("USCENTCOM," 2007). The most notable exception to CENTCOM's requirements is the lack of a high robustness capability. The following chapter provides an OB1 operational description and shows how OB1 will meet CENTCOM's requirement for high robustness.

THIS PAGE INTENTIONALLY LEFT BLANK

III. OB1 OPERATIONAL DESCRIPTION

A. CURRENT NETWORK ENVIRONMENT ("AS-IS")

CENTCOM's network architecture is a microcosm of the larger DoD network. CENTCOM users are required to access multiple networks in order to accomplish their mission. CENTCOM user required networks include:

- NIPRNET
- SIPRNET
- CENTRIXS-MCFI
- CENTRIXS-JCTF
- JWICS

Figure 4 shows a typical CENTCOM user workstation with multiple computer CPUs, keyboards, monitors and mice. Due to the current DoD requirement to have networks of varying classification air gapped, each individual user is required to have all this network architecture at their workstation. This particular network requirement significantly burdens the warfighter in areas such as:

- Expense of additional computers
- Expense of additional network architecture
- Expense of additional cooling requirements
- Expense of additional network administrative and maintenance personnel
- Additional time to install and maintain
- Excessive time requirements needed to deploy/re-deploy
- Lack of timely and pertinent information available to the warfighter

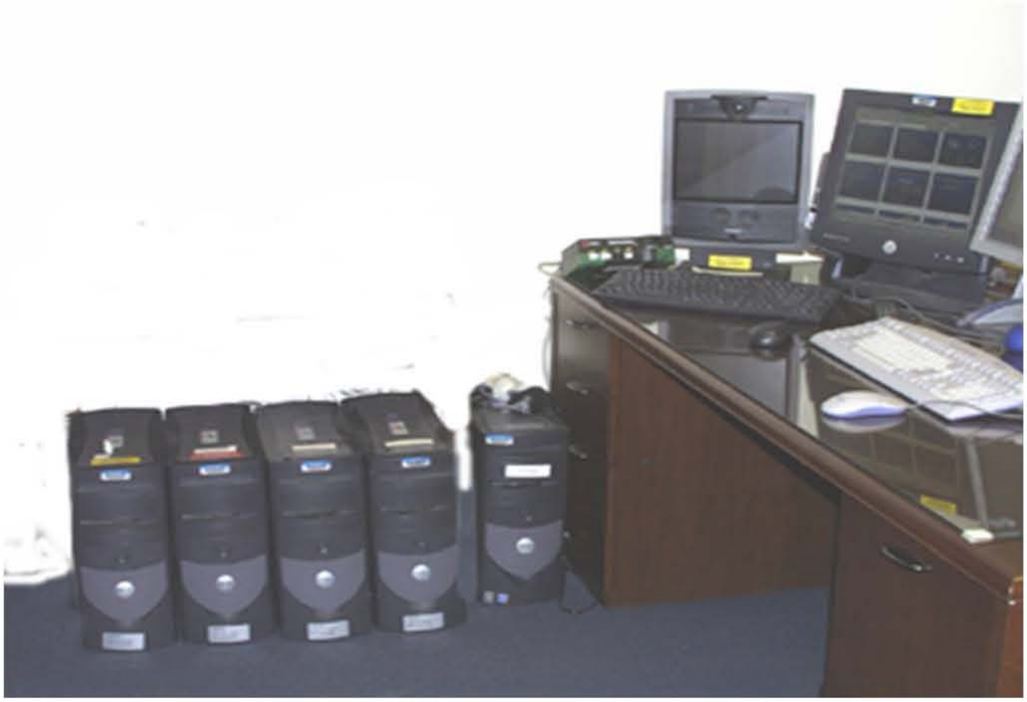


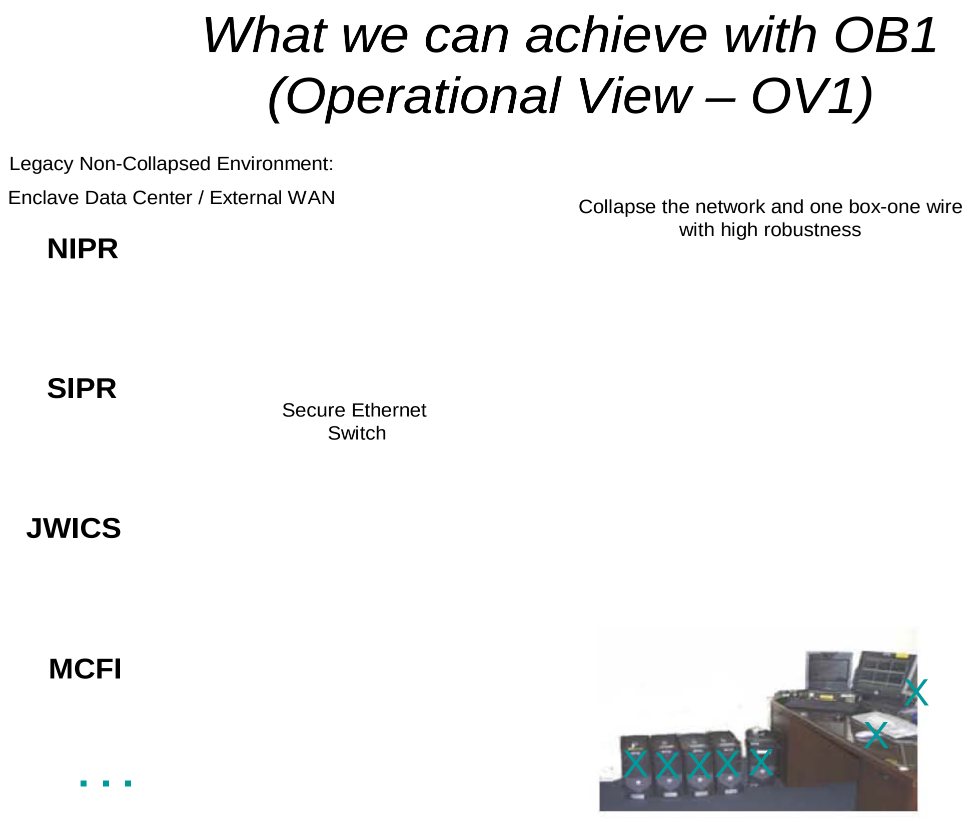
Figure 4. Typical Desktop Environment [From Network, Figure 2-1]

“The current mode of operation is to provide a desktop for each network. Each desktop is connected by fiber or CAT-5 cable to a distribution frame which connects to each of the data centers for each network. Type-1 encryption devices are used to interconnect enclaves (buildings, etc.). These networks range from UNCLASSIFIED to TOP SECRET. These components are generally replaced every three to five years as part of the life-cycle maintenance program. The cables from the desktops are within a “protected distribution system” (PDS). Data is encrypted when leaving the PDS and decrypted when re-entering the data center PDS” (Network, 2008, p. 3).

In order to function as a command and carry out its orders, CENTCOM often deploys teams of individual users to remote, unsecure locations. These locations are often in an unstable, high threat environment. Due to the amount of network equipment required, the current network infrastructure is not conducive to a rapid deploy/re-deploy tempo of operations under which CENTCOM operates.

B. NETWORK ENVIRONMENT WITH OB1 (“TO BE”)

The proposed OB1 architecture will allow for a single infrastructure of workstations, switches and cables (see Figure 5). This solution has multiple benefits on many different levels: less power consumption, easier to set-up/take down, easier to deploy/re-deploy and eases many network administrative burdens, i.e., adding/removing users from the network, adding/removing computers from the network, adding/removing networks to at a workstation. In their CONOPS, the OB1 team states, “This solution interoperates with legacy and coalition partner systems and allows for a rapid configuration of communities of interest (COI) without major physical changes to the network. This solution maximizes the use of our current IT investments” (Network Infrastructure, 2008, p. 5).



What we can achieve with OB1
(Operational View – OV1)

Legacy Non-Collapsed Environment:
Enclave Data Center / External WAN

Collapse the network and one box-one wire
with high robustness

NIPR

SIPR

Secure Ethernet
Switch

JWICS

MCFI

. . .

Figure 5. OB1 Operational View [From Network, Fig 2-2]

Figure 6 shows what a typical network architecture would look like with OB1. OB1 is not an attempt to modify the current way information is transferred across entire networks. What OB1 attempts to do is modify the last mile of the network infrastructure in such a way that reduces the burden of having a large network footprint that is not conducive to information sharing in a multinational environment.

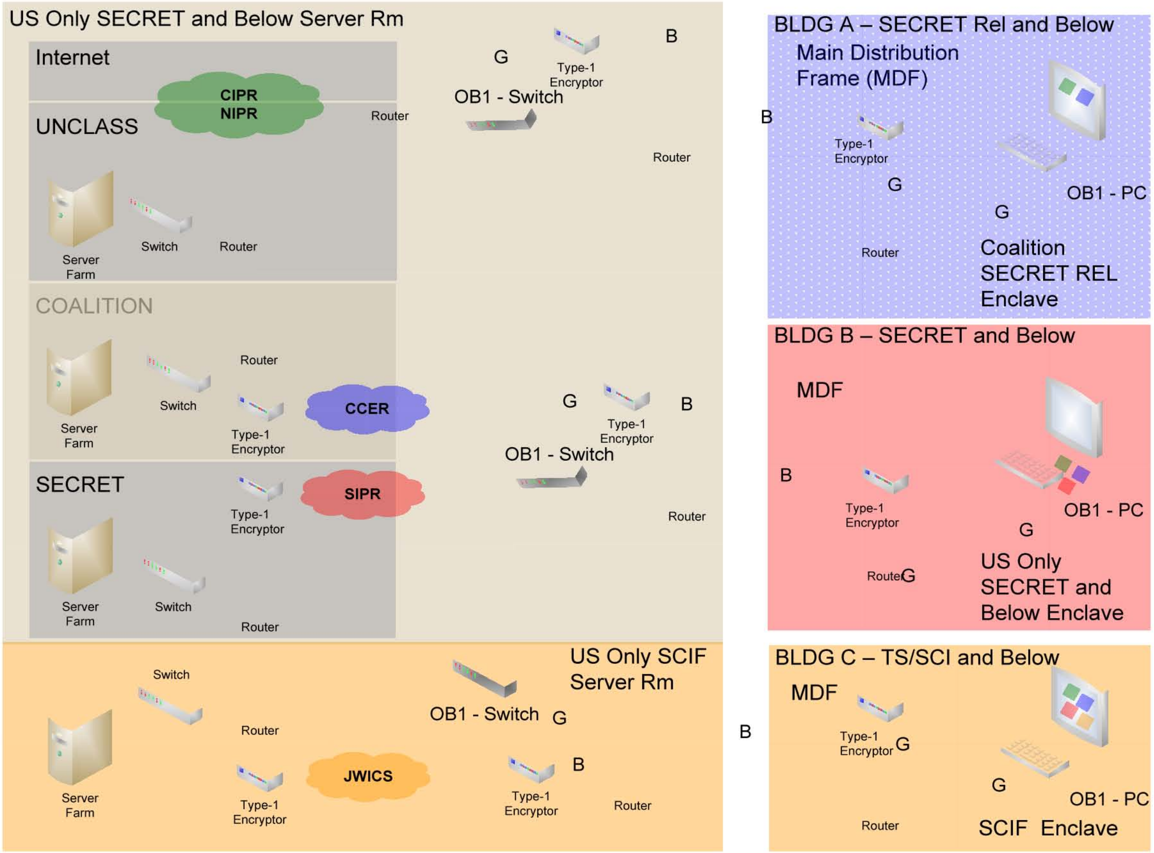


Figure 6. Typical OB1 LAN Architecture [From Network Infrastructure, Fig 3]

The primary components of OB1 consist of several technologies being developed by two primary vendors, Green Hills Software (GHS) and Objective Interface Solutions (OIS). Their products are:

- Green Hills Software
    - INTEGRITY® Operating System
    - INTEGRITY® Separation Kernel

- Objective Interface Solutions
    - Black Channel Gigabit Switch
    - Black Channel Network Interface Card (BC NIC)
    - Black Channel Administrator
    - Black Channel Authorizer

In Figure 6, the INTEGRITY® OS, Separation Kernel and BC NIC would reside on or in the CPU[5] (OB1-PC) associated with each monitor in the respected enclave. The three BC Gigabit switches are labeled “OB1-Switch” and they are located in the appropriate Server Rm (Farm).

Together, these four components allow a single user to access multiple networks of varying classification from a single workstation.

1. Cross Domain Solution

A cross domain solution (CDS) is defined as an information assurance solution that provides the ability to manually and/or automatically access and/or transfer between two or more differing security domains (CJCSI, p. GL-5). OB1 is not a CDS. According to the OB1 team the Unified Command Domain Management Office[6] (UCDMO) has termed OB1 as an access CDS. What that means is OB1 will not be able to transfer data directly from one security classification level to another i.e., have the ability to send and/or receive data from the SIPRNET while logged onto the NIPRNET and vice versa.

2. High Robustness

One of the major advantages and benefits of OB1 is its high robustness capability. CENTCOM uses chapter four of the Information Assurance Technical Framework (IATF) as their guidance for information assurance. The IATF defines what high

[5] OB1 is compatible with and intends to use legacy commercial off-the-shelf (COTS) CPUs.

[6] Established in July 2006. All DoD and Intelligence Community cross domain efforts now fall under their jurisdiction.

robustness is, as well as, other information assurance requirements that need to be met in order for a network architecture to achieve certain standardized levels of security.

The OB1 team using the IATF as guidance defines high robustness as proving to the maximum extent possible, that information is secure, even in high threat environment. For CENTCOM, a high threat environment would be defined as Afghanistan, Iraq or similar operating environments. Figure 7 shows where high robustness falls in a high threat level, high information type environment.

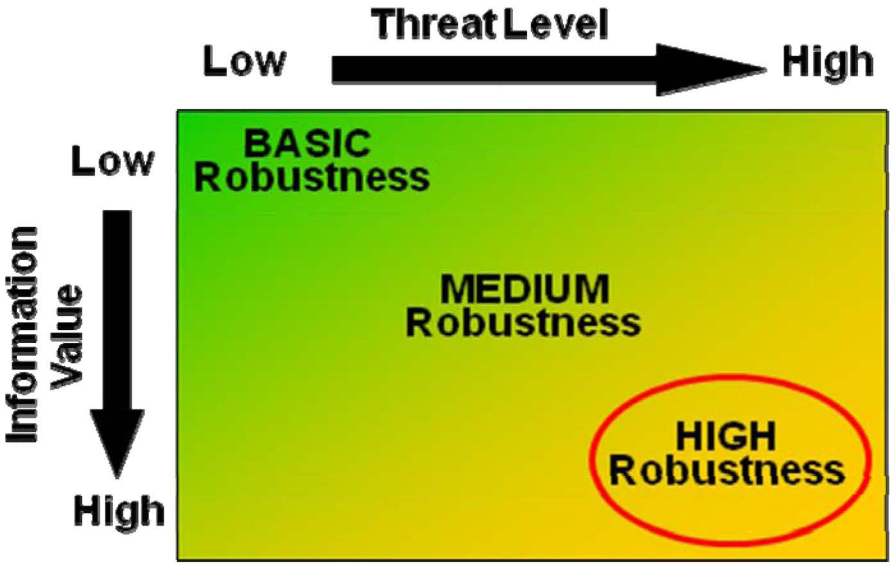


Figure 7. High Robustness Chart [From Staneszewski, Fig 3]

For the OB1 critical components (GHS and OIS vendor products) high robustness requires:

- Formal Methods Evaluation – mathematical proof that the component enforces security policy under all possible conditions
- Exhaustive testing – total test coverage, documentation of processes, requirements, and traceability
- Penetration testing by skilled NSA attackers

All testing, proofs, and processes are documented in a structured set of artifacts for use by Information Assurance evaluators, certifiers, and accreditors.

According to CENTCOM’s Requirements Statement dated October 2007, CENTCOM requires the capability to access separate networks on a single workstation connected to a single wire which is connected to a data center that stores information for those networks. Objectives of the new network architecture include reduced workstation and network infrastructure, a reduction in the requirement to air gap information across domains and the ability to interoperate with deployed Coalition partner systems. The solution must take into consideration the cost of development, implementation and certification, use of legacy systems and peripherals and it must strive to minimize disruption of the existing system. CENTCOM believes OB1 meets all of their stated requirements and objectives. An independent Business Case Analysis of OB1 will be used to help verify CENTCOMs belief that OB1 is, in fact, a viable solution.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. BUSINESS CASE ANALYSIS (BCA) DEFINED

A. BUSINESS CASE ANALYSES

The Defense Acquisition (DAU) website describes a BCA as "…a best-value analysis that considers not only cost, but other quantifiable and non-quantifiable factors supporting an investment decision. This can include, but is not limited to, performance, producibility, reliability, maintainability, and supportability enhancements." It is an important business tool that helps decision makers to evaluate alternative approaches and to decide on the allocation of scarce resources. The underlying purpose of a BCA is to evaluate the financial soundness of a proposed solution to a problem with a financial analysis that will supply the decision maker with one important piece of information that will be considered together with other factors that bear on the decision.

It is important to note that a BCA is an all-purpose commonly used term and may also be referred to as Cost/Benefit Analysis, Cost of Ownership Analysis, Economic Analysis or Return on Investment (ROI) Analysis. Each term implies a slightly different approach in answering the general question: "What are the likely financial and other business consequences if we take this or that action (or decision)?" Since none of these terms have a single precise or universally agreed upon definition, it is important to clarify our definition of a BCA.

In order to meet that objective, this thesis will model its BCA approach from that recommended by the DAU and summarized in a previous Naval Postgraduate School (NPS) thesis titled "A Methodical Approach for Conducting a Business Case Analysis for the Joint Distance Support and Response (JDSR) Advanced Concept Technology Demonstration (ACTD)," dated December 2006.

As a minimum a BCA should include:

- An introduction that states what the case is about and why it is necessary
- A statement specifying assumptions and constraints
- Identify possible alternatives and status quo

- An estimate of costs and benefits of each alternative
- A Sensitivity and risk analysis
- A conclusion and recommendations

Most financial analyses can be described as a four phase process, our BCA is no different. Figure 8 shows our BCA concept as defined by the DAU on their website.

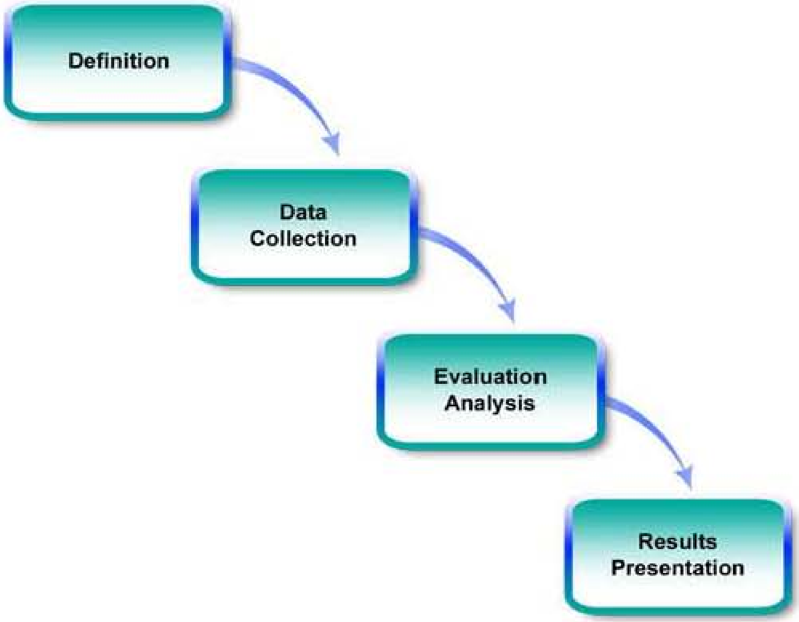


Figure 8. BCA methodology as defined by the DAU [From Defense, Fig 1-3]

1. Definition

In this phase, the scope of the analysis is defined. In order to do this, assumptions and constraints that will guide the analysis must be clarified. Analysts also identify the number of alternatives the BCA will consider. The definition stage can often make or break a BCA. It lays the groundwork for the BCA, communicating to decision-makers the reasoning of the analysts, which establishes the credibility of the BCA.

2. Data Collection

The plan will specify the types of data required, the potential data sources, and the approaches to obtain these data. Often times the data are difficult to obtain. It may be hidden in company’s databases accessible only to limited number of company personnel, it may be hidden deep in financial spreadsheets or, if it is a new technology, that data simply may not be available yet. In situations where the required data are not available, an estimate is made with the approach for calculating the estimate clearly explained and documented. There are several costs estimating approaches available: parametric estimation, analogy estimation and engineering estimation. Upon the completion of data collection, the data are examined for consistency and anomalies. Thereafter, the data are normalized to support “apple to apple” comparisons, such as adjustment for inflation/deflation to account for the time value of money.

3. Evaluation Analysis

In this phase, analysts do the actual breakdown of the data obtained in the data collection phase. Here, analysts build a case for each alternative using both qualitative and quantitative data. Each alternative is compared against the baseline to determine which one has the best overall value. Sometimes this can be extremely difficult, especially if comparing both quantitative data and qualitative data. One tool to help convert the data to a common baseline is the analytic hierarchy process (AHP). AHP is a process that assigns numerical values to different aspects of an alternative and eventually assigns an overall numerical score to each alternative. This process allows analyst to rank alternatives in order of preference.

Once all the data have been collected by the analyst, a risk analysis and sensitivity analysis should be done. A risk analysis attempts to predict the likelihood of an event occurring, and the potential impact of that on the case. A sensitivity analysis attempts to explain what happens if assumptions change or prove wrong, typical “What if” scenarios. A sensitivity analysis should show how sensitive your models’ overall outputs are to changes in input and how those changes impact the bottom line.

4. Results Presentation

The best analysis in the world is worthless if the results of that analysis cannot be clearly articulated to the decision-makers. Conclusions should state the results of the analysis clearly and succinctly as supported by previous evidence. Effective conclusions are based on the upfront stated objectives. It is here that analysts should explain any unexpected results or findings that could be misinterpreted.

Throughout the BCA process quantitative data should be expressed in charts and graphs. One should not expect decision-makers to labor through the analytic process attempting to ascertain the results of analysis on their own. The analysts should tell them exactly what is meant and why.

An effective BCA must also contain a recommended course of action (COA) for the decision-makers. The BCA should provide reasonable support to back up analysts recommendations; enough support that the average person would find compelling. A recommendation should bring closure to the analysis by reminding the reader the analytic part of the BCA process is done and the future of the project, the way ahead, is once again up to them.

B. WORK BREAKDOWN STRUCTURE (WBS)

A WBS has a hierarchical tree structure that captures all the work of a project in an organized way. A WBS can be product or process oriented based on the ultimate end-items of the project. The Department of Defense handbook (MIL-HDBK-881, 2005) had defined WBS as:

> A WBS displays and defines the product, or products, to be developed and/or produced. It relates the elements of work to be accomplished to each other and to the end product. A WBS can be expressed down to any level of interest. However the top three levels are as far as any program or contract need go unless the items identified are high cost or high risk. Then, and only then, is it important to take the work breakdown structure to a lower level of definition.

There are several benefits to having a WBS planned out properly for a project. A WBS helps to keep track of the schedule, resource allocation, cash flow, expenditures, and performance of the project. Another goal is to provide a systematic and standardized method for gathering cost data across all programs. Having actual historical data to support cost estimates of similar defense materiel items is a valuable resource.

C. NET PRESENT VALUE (NPV) ANALYSIS

Net Present Value of an investment is defined as the sum of the present values of the annual cash flows. The annual cash flows are the Net Benefits (revenues minus costs) generated from the investment during its lifetime. These cash flows are discounted or adjusted by incorporating the uncertainty and time value of money. An investment with the larger NPV is a better option. The formula for calculating NPV is as follows:

$$NPV = \sum_{t=1}^{n} \frac{C_t}{\left(1+r\right)^t}$$

where

t – the time of the cash flow

n – the total time of the project

r – the discount rate

C_t – the net cash flow at time

Discount rate is the rate used to discount future cash flows to their present values. An approach to choosing the discount rate factor is to decide the rate which the capital needed for the project could return if invested in an alternative venture. For our analysis of OB1, a discount rate of 3% was chosen for the baseline computation, because that is the current return of 10-year U.S. Treasury notes. This factor is in accordance with the instruction from Office of Management and Budget, which instructs U.S. government investment analyses to use a discount factor equal to the interest rate on U.S. Treasury notes whose duration equals the duration of the investment being analyzed.

D. RETURN ON INVESTMENT (ROI) ANALYSIS

Return on Investment (ROI) measures the ratio of money gained or lost on an investment relative to the amount of money invested. An Annualized ROI is used here to calculate the investment over a certain period. An investment with a higher annualized ROI is a better investment option than an investment with a lower annualized ROI. For our case, we are interested in an Annualized ROI over a period of 13 years.

E. PAYBACK PERIOD

Payback period answers the question of “When does the investment pay for itself?” It occurs at the point where the cumulative cash inflows are equal to the cumulative cash outflows, i.e., no net loss or gain.

F. SENSITIVITY ANALYSIS

A sensitivity analysis is a process of varying the input parameters of a model over a reasonable range and observing the relative change in the model output. The purpose of the sensitivity analysis is to determine the sensitivity of a model result to uncertainty in the input data, as in the case of financial analyses evaluating multiple alternatives where an uncertain assumption might change the selection of a recommended alternative. In cases such as those, the assumption is allowed to generate data at the upper and lower bounds of its confidence interval to test whether or not the recommendation supported by the basic assumption would be changed by modifying the values of the financial data that are based on the assumption.

V. OB1 BUSINESS CASE ANALYSIS

A. OB1 WORK BREAKDOWN STRUCTURE (WBS)

The top level WBS for the OB1 JCTD consists of Investment and Operations and Support. These WBS elements are described in the paragraphs below.

1. Investment

The investment for OB1 consists of

- Design, development, test and evaluation of GHS INTEGRITY® secure operating system and separation kernel
- Objective Interface Solution's Black Channel NICs and switches
- Software and hardware integration and configuration
- Robustness certification for the INTEGRITY® PC and OIS's Black Channel NIC and switch

2. Operations and Support (O&S)

The O&S consists of

- Upgrading or replacing all hardware and/or software on a recurring basis as deemed appropriate by individual commands. For our evaluation we used the CENTCOM recommended refresh cycle of three years.
- Administrative and maintenance personnel. For our evaluation we used CENTCOM recommended numbers based on the size of their network.

B. ANALYSIS OF CENTCOM DATA

The following sections provide a financial analysis of the cash flows that result from investing in OB1 and then operating and supporting it. Baseline estimates for the cash flows were supplied by CENTCOM's OB1 team. Additional data are the professional judgments myself and my thesis advisor. Complete data can be found in Appendix A and B. All costs are in FY 09 unless otherwise stated.

1. Net Present Value (NPV) Analysis

Our base case analysis for OB1 assumes a three-year implementation phase in which OB1 will complete research and development, including test and evaluation, robustness and integrity (Information Assurance (IA)) certifications and other accreditations and certifications. We estimate these implementation phase, non-recurring investment costs at $13.7M for year one, $12.9M for year two and $9.3M for year three.

Our base case analysis assumes FY 2009 dollar values; other base case parameters include a discount factor (df) of 3% and a recurring investment[7] of $1.8M every three years (assuming a three year refresh cycle).

The investment and savings data in the following NPV tables were obtained from the CENTCOM OB1 team. See Appendix A and B for further details. The tables below show a detailed analysis of the data provided by CENTCOM.

Specifically, NPV is computed using the following formula:

$$NPV = \sum_{t=1}^{n} \frac{C_t}{(1+r)^t}$$

where

t – the time of the cash flow

n – the total time of the project

r – the discount rate

C_t – the net cash flow at time

Specifically, t = 1, 2, 3…13, n = 13, r = 0.03 and C = NPV Savings year 1, year 2, year 3…year 13. As shown in Table 2, over 13 years, we find that our base case analysis of OB1gives us a NPV Savings of $263.1M.

[7] The recurring investment comes from the upgrade and replacement of the OB1 Network Architecture every three years (CENTCOMM recommendation).

Base Case Plus $0.0M Additional Non-Recurring Investment

	Remaining N-R Investment			Recurring Investment + O&S Savings ($M)									
	Year 1	2	3	4	5	6	7	8	9	10	11	12	13
Investment	-13.7	-12.9	-9.3	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8
Savings	0.0	0.0	0.0	25.7	15.9	23.9	102.7	31.9	31.9	102.7	31.9	31.9	102.7
Net Savings	-13.7	-12.9	-9.3	23.8	15.9	23.9	100.9	31.9	31.9	100.9	31.9	31.9	100.9

NPV Savings ($M)

df %	Year 1	2	3	4	5	6	7	8	9	10	11	12	13	NPV Savings
3%	-13.7	-12.5	-8.8	21.8	14.2	20.6	84.5	25.9	25.2	77.3	23.7	23.0	70.7	263.1
5%	-13.7	-12.3	-8.5	20.6	13.1	18.7	75.3	22.6	21.6	65.0	19.6	18.6	56.2	183.9
10%	-13.7	-11.7	-7.7	17.9	10.9	14.8	56.9	16.3	14.9	42.8	12.3	11.2	32.1	76.2

Table 2. OB1 NPV after 13 years with $0.0M Additional Non-Recurring Initial Investment

NPV Savings (13yrs) = $263.1M

We can also see from Table 2 that in year four (the first year of OB1 implementation at CENTCOM), using a 3% df, that we have NPV Savings of $21.8M. This tells us that OB1 saves money from its first year of implementation. It should be noted that OB1 is assumed to use the Life Cycle Replacement method[8] for implementation. Thus, for our analysis, we phased in the benefits of OB1. Specifically, in year four we assumed OB1 would only achieve a 25% savings, year five 50%, year six 75%, and finally, OB1 will reach its full savings potential in years seven and beyond.

At CENTCOM most of the network architecture gets replaced every three years. Since, one of the primary objectives that OB1 achieves is the consolidation of multiple networks (NIPR, SIPR, JWICS, etc) OB1 provides a much smaller footprint than the current network architecture. Because of this smaller footprint, OB1 obtains a large amount of savings (in hardware, software, personnel) every third year (years 7, 10, 13, etc). Consequently, we expect the savings of OB1 to be even more compelling over a period of 23 years than over 13.

Using the same formula as above for NPV, from Table 3 we can see that, with a 3% df over a period of 23 years, OB1 yields a NPV savings of $444.7M.

[8] With the Life Cycle Replacement method legacy systems will be swapped out with OB1 when the legacy systems are normally scheduled for replacement.

	Base Case Plus $0.0M Additional Non-Recurring Investment																							
	Remaining N-R Investmen			Recurring Investment + O&S Savings ($M)																				
	Year 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
Investment	-13.7	-12.9	-9.3	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8	0.0	0.0	-1.8	0.0	
Savings	0.0	0.0	0.0	25.7	15.9	23.9	102.7	31.9	31.9	102.7	31.9	31.9	102.7	31.9	31.9	102.7	31.9	31.9	102.7	31.9	31.9	102.7	31.9	
Net Savings	-13.7	-12.9	-9.3	23.8	15.9	23.9	100.9	31.9	31.9	100.9	31.9	31.9	100.9	31.9	31.9	100.9	31.9	31.9	100.9	31.9	31.9	100.9	31.9	
	NPV Savings ($M)																							
df %	Year 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	NPV Savings
3%	-13.7	-12.5	-8.8	21.8	14.2	20.6	84.5	25.9	25.2	77.3	23.7	23.0	70.7	21.7	21.1	64.7	19.9	19.3	59.2	18.2	17.6	54.2	16.6	444.7
5%	-13.7	-12.3	-8.5	20.6	13.1	18.7	75.3	22.6	21.6	65.0	19.6	18.6	56.2	16.9	16.1	48.5	14.6	13.9	41.9	12.6	12.0	36.2	10.9	276.1
10%	-13.7	-11.7	-7.7	17.9	10.9	14.8	56.9	16.3	14.9	42.8	12.3	11.2	32.1	9.2	8.4	24.1	6.9	6.3	18.1	5.2	4.7	13.6	3.9	94.9

Table 3. OB1 NPV after 23 years with $0.0M Additional Non-Recurring Initial Investment

NPV Savings (23yrs) = $444.7M

C. RETURN ON INVESTMENT (ROI)

ROI is computed over a period of 13 years as the base case and over 23 years as an excursion. The base case discount factor remains at 3% with an initial non-recurring investment of $13.7M for year one, $12.9M for year two and $9.3M for year three. The recurring investment cost is assumed to be $1.8M every three years starting at year four. The annualized ROI is computed using the formula:

$$\text{ROI} = \frac{\text{NPV Savings}}{\text{NPV of Investment}} \text{X100}$$

Therefore, over a period of 13 years with a NPV savings of $263.1M and a NPV of investments of $39.7M our base case analysis of OB1 yields a ROI of 662.9%. Taking the analysis of OB1 out another 10 years to 23, using a NPV savings of $444.7M and a NPV of investments of $42.8M our base case analysis of OB1 yields a ROI of 1,038.7%.

Base Case Annualized ROI (13yrs) = 662.9%

Base Case Annualized ROI (23yrs) = 1,038.7%

From Figure 9, we can see OB1 cash flow over 23 years shows, that after the initial investment costs of developing OB1, we have a consistent positive return on cash flow. There is a spike every three years due, primarily, to the large savings in network infrastructure replacement.

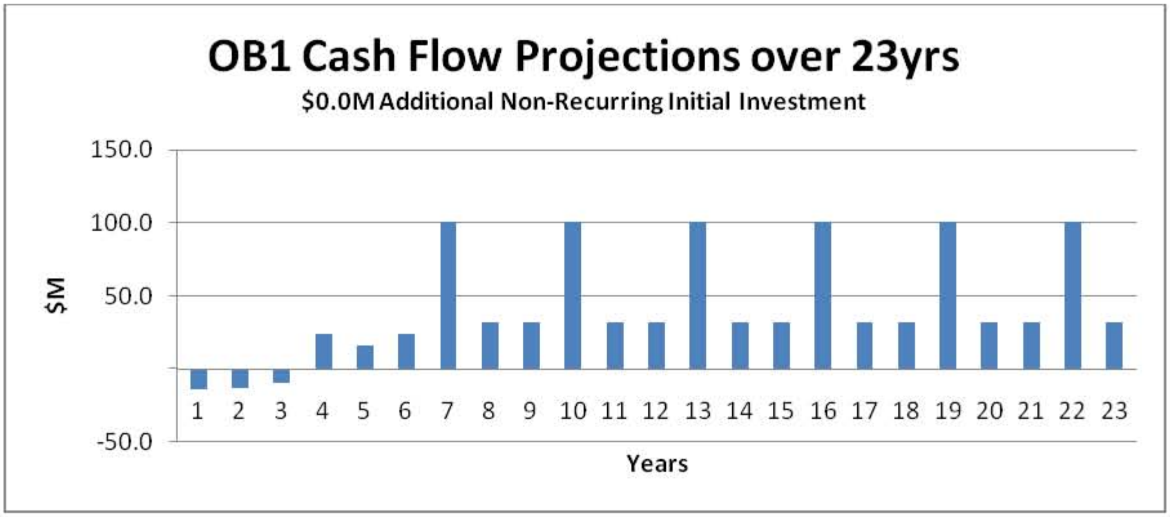


Figure 9. OB1 Cash Flow Projection over 23 years ($0.0M Add'l NRI)

D. SENSITIVITY ANALYSIS

Sensitivity analyses were conducted on three key variables in the analysis: the initial non-recurring investment amount, the recurring investment of OB1 after implementation, and the discount factors. Modifying one of these values at a time, while maintaining the others constant, provides a useful analytical tool for understanding the financial behavior of the OB1 JCTD.

1. Varying the Amount of Non-recurring Initial Investments

The CENTCOM estimated initial investment costs for OB1 were $35.9M. Figures 10 and 11 show that by increasing the initial non-recurring investment in OB1($39.7M) from $10.0M more, and $20.0M more respectively, we still have positive cash flows beginning in year four. Figures 10 and 11 also continue to show positive cash flows throughout the life of OB1. Thus, we can say that OB1 is a viable alternative to the current solution even if initial investment in OB1 is off by a factor of nearly two.

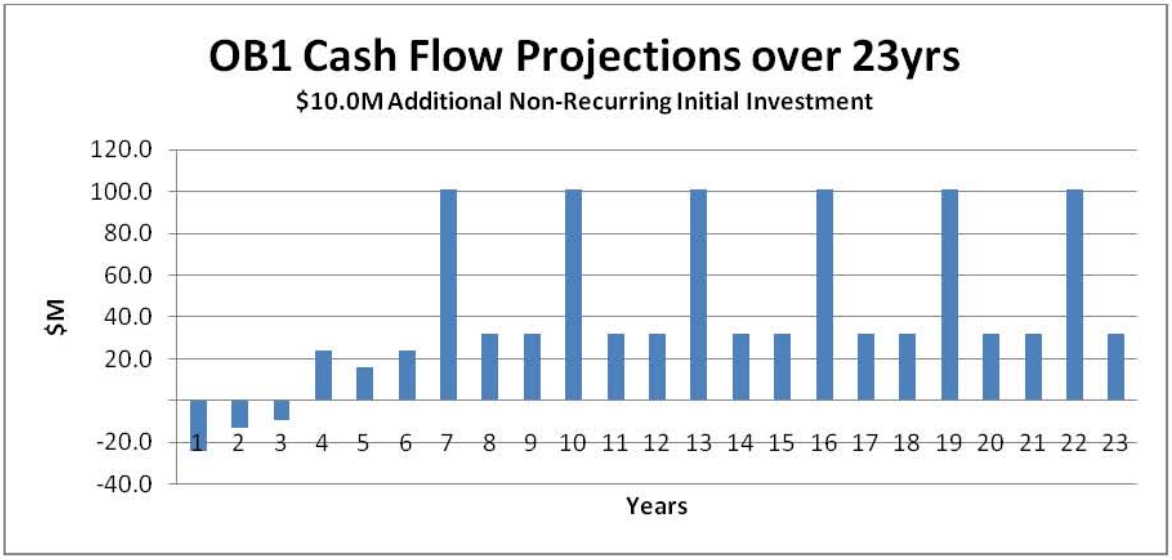


Figure 10. OB1 Cash Flow Projection over 23 years ($10.0M Add'l NRI)

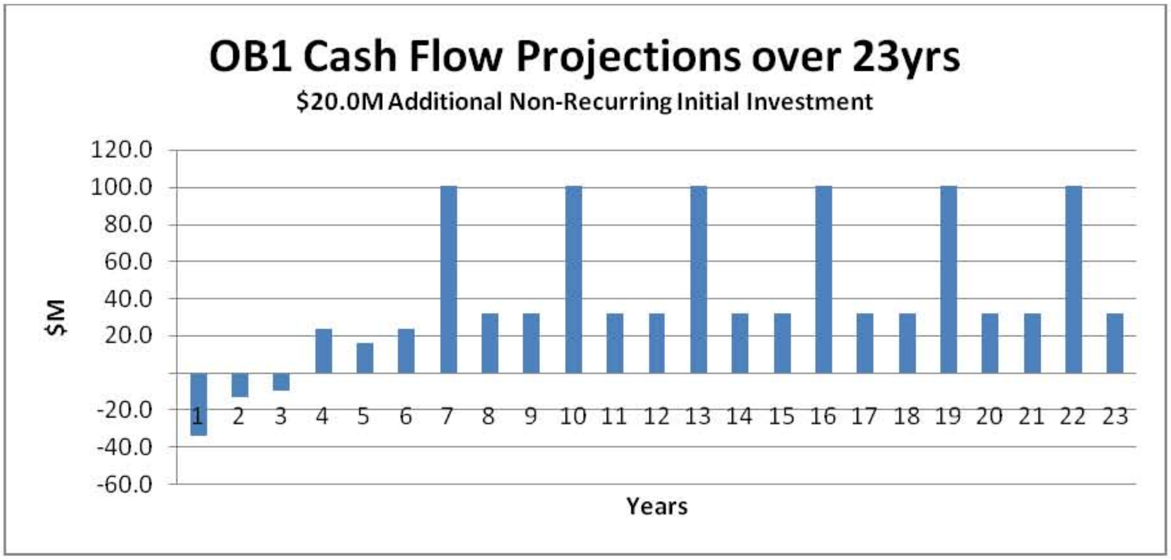


Figure 11. OB1 Cash Flow Projection over 23 years ($20.0M Add'l NRI)

A further analysis of OB1 can be seen in Figures 12 and 13. Figure 12 displays the NPV from the cash flows in Figure 10. Similarly, Figure 13 shows the NPV from the cash flows in Figure 11.

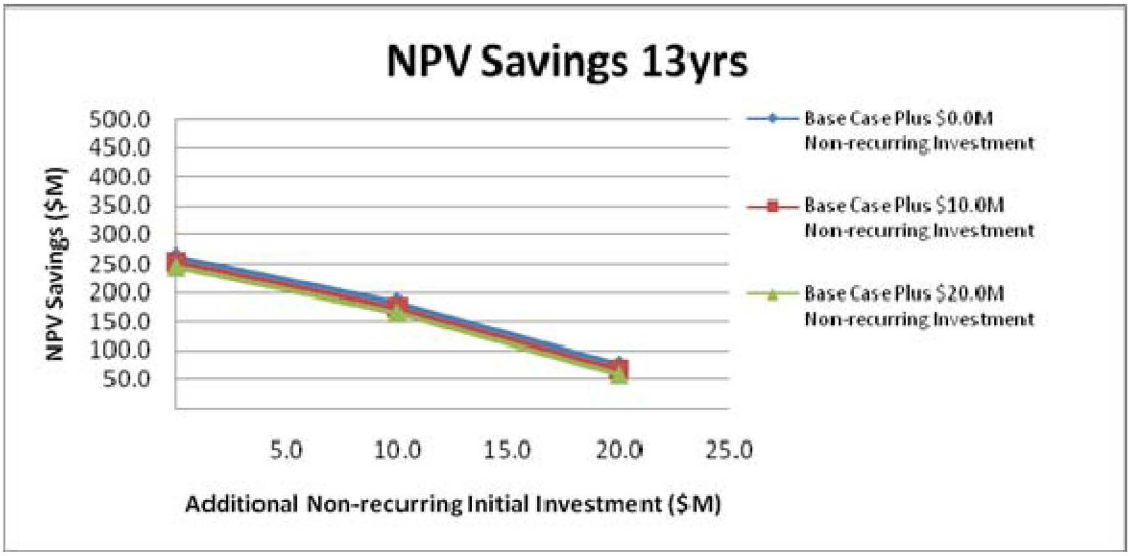


Figure 12. OB1 NPV Savings over 13 years

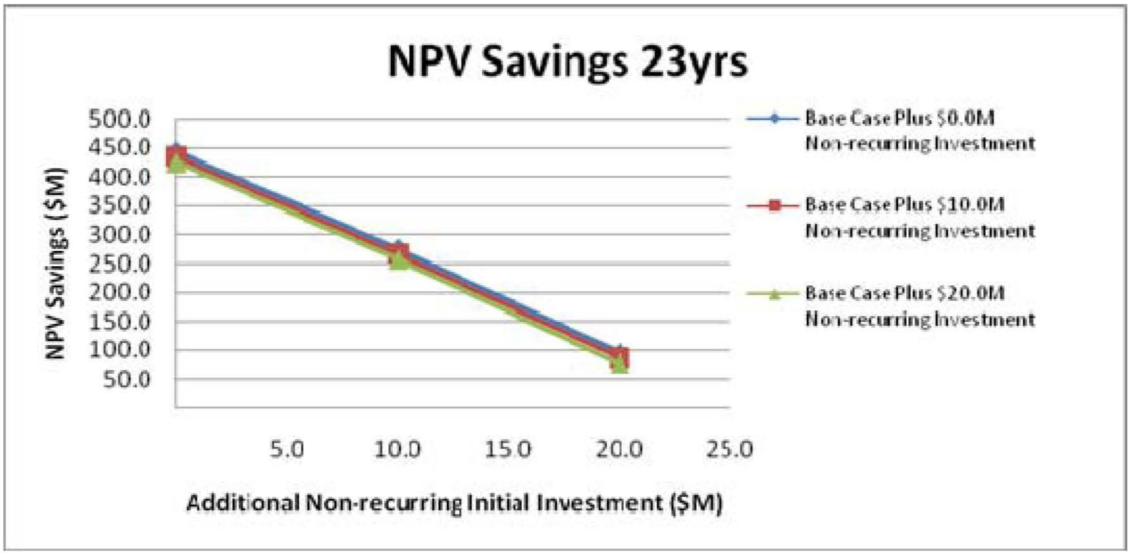


Figure 13. OB1 NPV Savings over 23 years

From the analysis of Figures 12 and 13 we can see that OB1 has a positive NPV Savings over 13 years, and 23 years, even if the initial investment cost for fielding OB1 is $10.0M or $20.0M more than originally budgeted ($35.9M) over three years.

The results of converting the NPV analyses above to ROI are shown in Figure 14. We see that as initial investment increases, ROI decreases. An overall positive ROI is still obtained given our worst case scenario ($20.0M investment over 23 years).

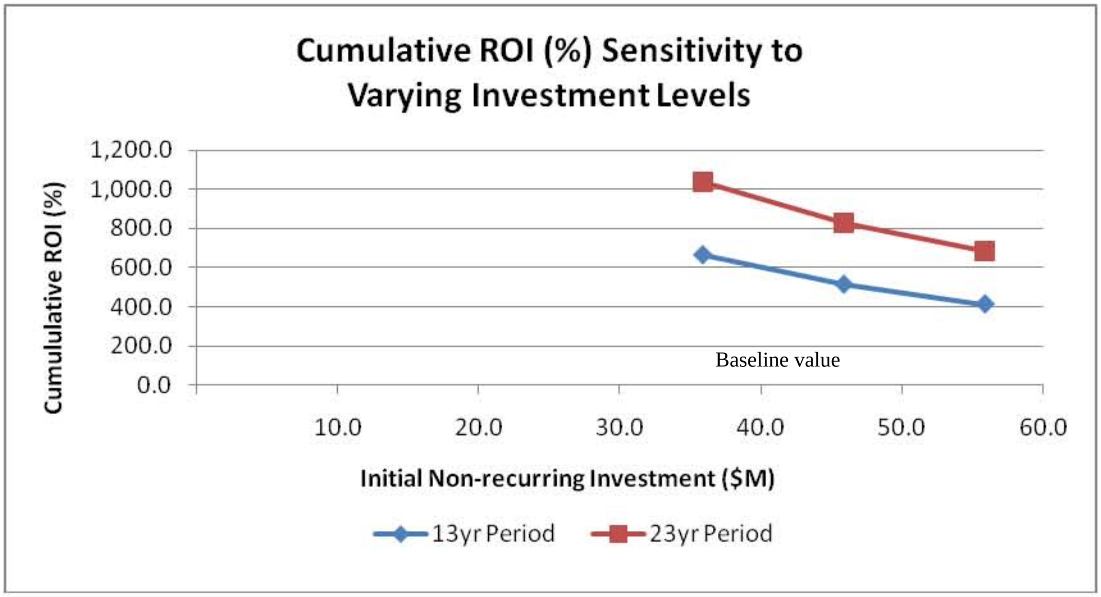


Figure 14. Cumulative ROI (%) Sensitivity to Varying Investment Levels

2. Sensitivity Analysis on Recurring Investment

This paragraph addresses the sensitivity analysis of OB1’s ROI to varying levels of recurring investment. Our base case analysis of OB1 assumes a $1.8M recurring investment for OB1 over its life span. This recurring investment comes from network architecture upgrades, including, desktop PCs, monitors, BC NICs, BC switches, upgraded cabling, software licenses and system certifications and/or re-certifications.

In this sensitivity analysis, we compute ROI for recurring investments in a range from -50% of our baseline value of $1.8M through 1000% of that value.

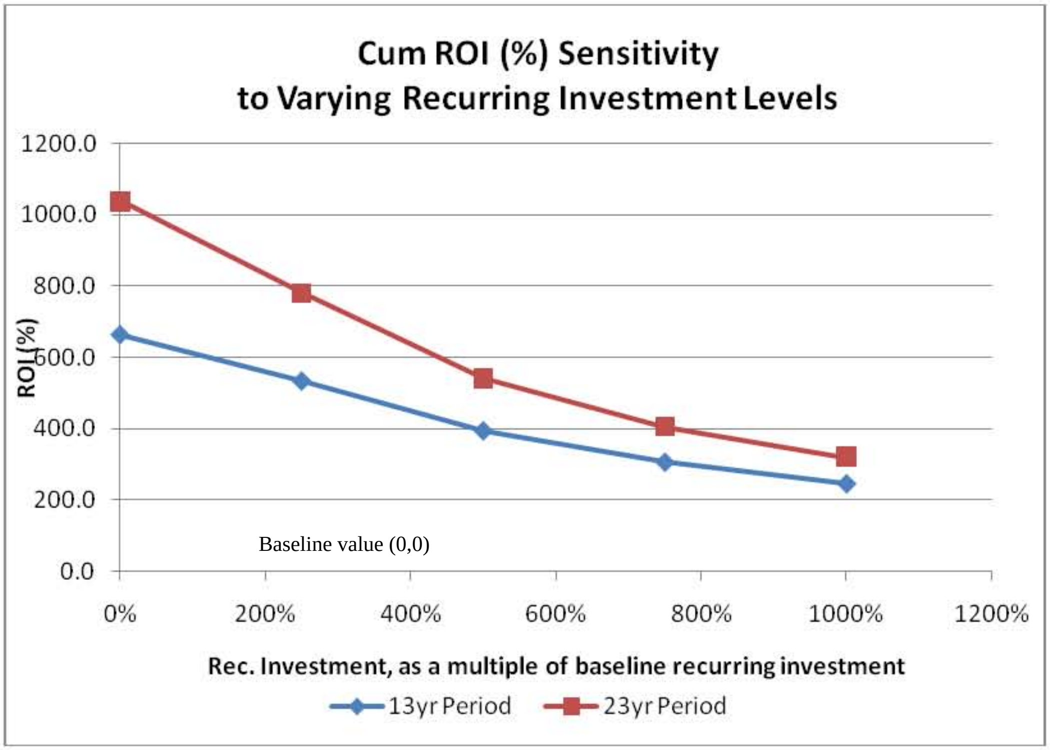


Figure 15. Cumulative ROI (%) Sensitivity to Varying Recurring Investment Levels

From Figure 15, we can see that even if the recurring investment estimate is off as much as 1000% ($18.0M vice $1.8M recurring) OB1 still has a positive ROI. Table 4 below shows these same results in tabular format.

Recurring Investment ($M)	R-I (%)	ROI ($M) (13 yrs)	ROI ($M) (23 yrs)
1.8	0%	662.9	1038.7
4.5	250%	533.3	780.2
9.0	500%	394.1	540.4
13.5	750%	306.3	405.8
18.0	1000%	245.9	319.6

S/A on R-I

Table 4. %ROI obtained over varying recurring investments. Assumes a 3% df and $0.0M Nonrecurring Investment

3. Varying % of Discount Factor

Our base case analysis used a discount rate on a 10-year Treasury note of 3%. Thus, there is a lot of potential for inflation to weaken the future outlook of OB1. We analyzed OB1 ROI for discount rates of 3%, 5% and 10%.

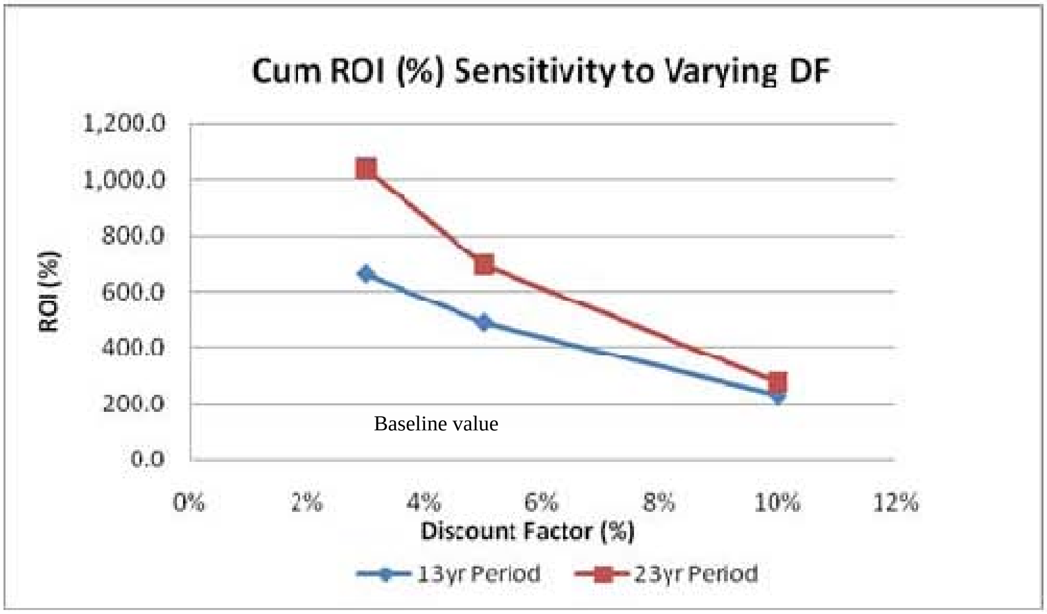


Figure 16. Cumulative ROI (%) Sensitivity to Varying Discount Rates

Figure 16 shows that even if the discount rate increases, from 3% to 10%, OB1 is a robust solution.

This BCA described a detailed WBS, analysis of CENTCOM provided data and sensitivity analysis. The following chapter will summarize the results of this analysis.

VI. CONCLUSION AND RECOMMENDATIONS

This report presented an overview of the OB1 JCTD, the OB1 technology itself, comparative alternative technologies to OB1, a generic structure to use as a guideline for performing BCAs, and the application of that generic BCA structure to the OB1 JCTD.

The BCA compared the current DoD military network architecture ("as-is") to what could be achieved ("to-be") with the OB1 technology. Life Cycle Costs consists of investment cost to develop OB1, as well as, the cost to upgrade, administrate and maintain it.

The key results of the business case analysis are summarized as follows:

A. OVERVIEW

- The OB1 technology is not a new network topology. It is merely modifying the existing network in a way that reduces the network footprint, streamlines the process of network set-up and take-down, helps ease the burden of adding and removing users to/from the network and, perhaps most important, provides more current and timely information to the warfighter.
- This thesis does not in any way analyze whether the OB1 technology is capable of being built or if it meets DoD networking security requirements, especially, regarding classified information.

B. FINANCIAL ANALYSIS

A sample of the cost benefits achieved from OB1 is contained in Table 5. As we can see from the table OB1 has the potential for a savings of $2,656.1M over a 23-year life cycle of OB1. That is a 95.6% savings over the current architecture.

LCCE (23yrs)				
	As-Is ($M)	OB1 ($M)	Delta $	Delta %
Investments	1,294.7	48.7	1,246.1	96.2%
O&S	1,482.3	72.3	1,410.0	95.1%
Total	2,777.0	121.0	2,656.1	95.6%

Table 5. Life Cycle Cost Estimate (LCCE) for OB1 (23 years)

Table 6 shows NPV and ROI for our base case analysis assuming:

- 10 year life cycle for OB1
- Discount factor of 3%
- $35.9M initial non-recurring investment
- $1.8M recurring investment.

NPV	ROI
$263.1M	662.9%

Table 6. NPV and ROI for our base case analysis

Using our base case scenario of a 10-year life span for OB1, a discount factor of 3%, $35.9M initial non-recurring investment and a $1.8M recurring investment OB1 will yield a NPV of $263.1M and a ROI of 662.9%.

C. SENSITIVITY ANALYSIS

- The base case annualized ROI never falls below 275.6% when the discount factor was varied from 3% to 10%
- The base case annualized ROI does not fall below 683.4% even when the initial investment cost to field OB1 is increased by $20.0M dollars
- The base case annualized ROI does not fall below 231.7% even when varying the recurring investment costs from 0% to 1000%
- OB1 yields a ROI of 49.9% even under a worst case scenario:
    - 10-year life of program
    - 10% discount factor
    - Additional non-recurring investment of $20.0M
    - 1000% ($18.0M) increase in recurring costs (O&S)

D. RISK ANALYSIS

- The real risk involved with OB1 is the potential for it not to be able to perform as advertised. Specifically:

- Will OB1 be able to consolidate multiple independent levels of security (MILS) (i.e. multiple networks NIPR, SIPR, JWICS etc) onto one workstation
- And if it is capable of doing this, will it be able to enforce all the applicable DoD security requirements regarding the handling and separation of classified material

E. BOTTOM LINE

The analysis conducted in this thesis shows that OB1 is a financially viable and robust solution to the problem of having multiple air gapped networks. OB1 provides a high return on investment over a wide range of varying input factors and appears to be a worthwhile investment for the DoD.

F. RECOMMENDATIONS FOR FUTURE RESEARCH

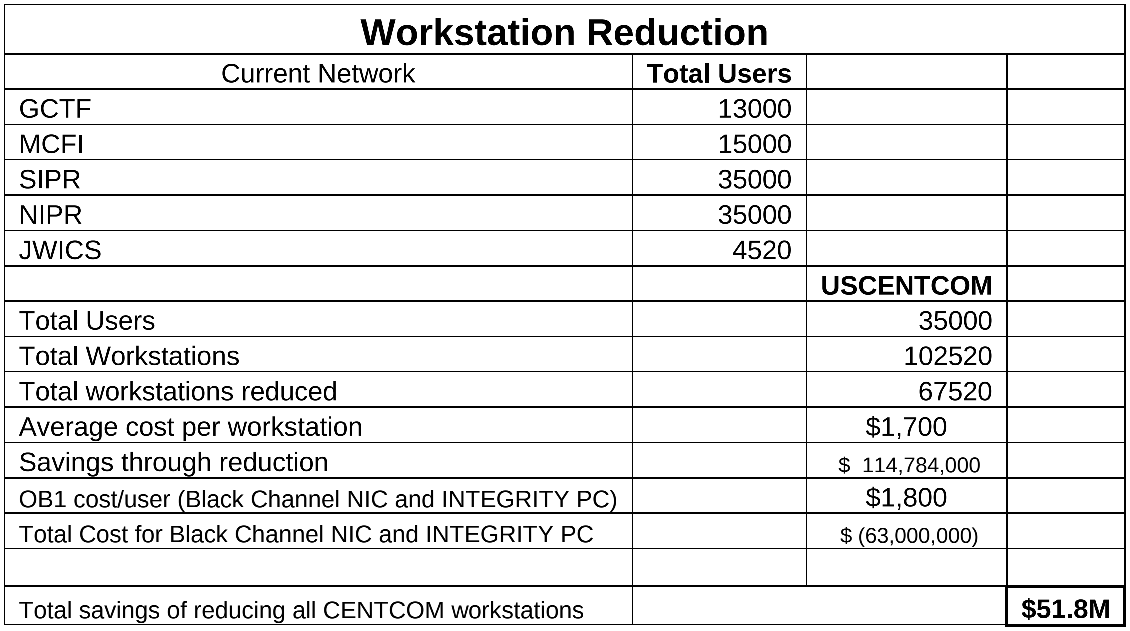
The technology required in order to consolidate multiple air gapped networks, while maintaining security via data separation, is extremely technical and difficult to do. However, there are many vendors and government entities that have made significant strides in this area of research over the last couple of years.

One area of future research is the potential benefits that OB1 could bring to a command via improved knowledge management (KM) and knowledge superiority (KS) practices. Another area to be researched could be the benefits of thin client computing. OB1 has the ability to provide either thin client, thick client computing or any combination thereof. Thin client computing by itself holds several advantages for an organization. These advantages combined with the added benefits of better KS/KM have the potential to make OB1, or any other similar technology, extremely appealing to a command, organization and, ultimately, warfighter.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

The following data were obtained from the OB1 team and used extensively in this BCA.



Workstation Reduction

Current Network	Total Users		
GCTF	13000		
MCFI	15000		
SIPR	35000		
NIPR	35000		
JWICS	4520		
		USCENTCOM	
Total Users		35000	
Total Workstations		102520	
Total workstations reduced		67520	
Average cost per workstation		$1,700	
Savings through reduction		$ 114,784,000	
OB1 cost/user (Black Channel NIC and INTEGRITY PC)		$1,800	
Total Cost for Black Channel NIC and INTEGRITY PC		$ (63,000,000)	
Total savings of reducing all CENTCOM workstations			**$51.8M**

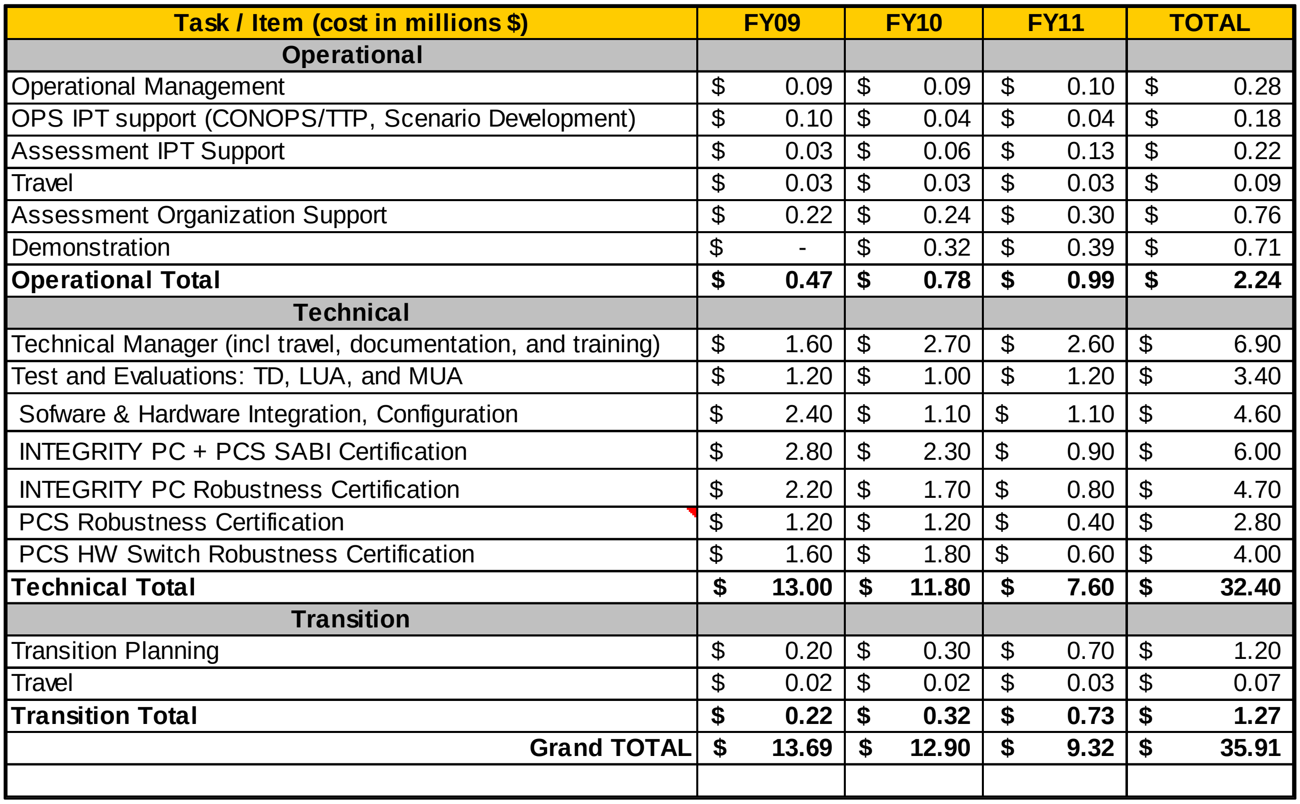
Network Equipment Reduction				
Current Network	Total			
GCTF	271			
MCFI	313			
SIPR	729			
NIPR	729			
JWICS	94			
# workstations per switch		48		
Savings factor		34%		
Value of COTS switch		$ 5,000		
Total switch savings All CENTCOM				**$3.6M**
Black Channel (BC) Switch and Administration and Authority Workstations				
# of workstations/ BC switch - est workstations per subnet		225		
# of BC switches required CENTCOM		156		
Cost of Black Channel Switch		$ 4,000		
Total Cost for BC Switches CENTCOM			**$-0.6M**	
# of BC Admin Workstations/User Workstation		500		
# of BC Admin Workstations required CENTCOM		70		
Administration Workstation Cost		$ 10,000		
Total Cost BC Admin Workstations CENTCOM			**$-0.7M**	
# of Authority workstations required (est 1 primary & 1 backup)		2		
Black Channel Authority Workstation Cost		$ 250,000		
Cost of Black Channel Authority Workstations			**$-0.5M**	
Total BC Switches, Admin and Authority Workstations CENTCOM				**$-1.8M**
Total Network equipment savings CENTCOM				**$1.8M**
Total hardware savings CENTCOM				**$53.6M**

Network Admin personnel Reduction				
Network	Total			
GCTF	26			
MCFI	30			
SIPR	70			
NIPR	70			
JWICS	9			
# workstations/network admin personnel		500		
Loaded labor cost		$ 130,000		
Savings factor matches % of reduced network hardware		34%		
Total network personnel savings CENTCOM		$ 8,700,488	over 3 yrs	**$26.1M**
PC Admin/Maintenance personnel Reduction				
Network	Total			
GCTF	52			
MCFI	60			
SIPR	140			
NIPR	140			
JWICS	18			
# workstations/PC admin/maint personnel		250		
Loaded labor cost		$ 110,000		
Savings factor - matches percentage of eliminated w/s		34%		
Total PC admin/maint personnel savings CENTCOM	$ 15,396,996	over 3 yrs		**$46.2M**
Total Personnel Saving CENTCOM				**$72.3M**
NOTE: Costs are based on CONUS (TAMPA) costs not the cost of personnel deployed.				

Base Operating Systems Costs				
Avg annual **electricity/workstation**	$ 201	over 3 years		$40.7M
Avg annual **air conditioning/workstation**	$ 92	over 3 years		$18.6M
Avg annual **costs for space/workstation**	$ 50	over 3 years		$10.1M
Workstation **wiring cost/workstation**	$ 100	cost/workstation - one time savings		$6.8M
BOS savings of all CENTCOM				**$76.2M**
NOTE: BOS does NOT include: • Lift/deployment costs • Type 1 Encryptor savings NOTE: Ambient Heat differential in desert AOR is greater than the Tampa factor used here				
Total savings reducing CENTCOM with OB1				**$202.1M**

APPENDIX B

Projected initial non-recurring investment costs as reported by the OB1 team.



Task / Item (cost in millions $)	FY09	FY10	FY11	TOTAL
Operational				
Operational Management	$ 0.09	$ 0.09	$ 0.10	$ 0.28
OPS IPT support (CONOPS/TTP, Scenario Development)	$ 0.10	$ 0.04	$ 0.04	$ 0.18
Assessment IPT Support	$ 0.03	$ 0.06	$ 0.13	$ 0.22
Travel	$ 0.03	$ 0.03	$ 0.03	$ 0.09
Assessment Organization Support	$ 0.22	$ 0.24	$ 0.30	$ 0.76
Demonstration	$ -	$ 0.32	$ 0.39	$ 0.71
Operational Total	**$ 0.47**	**$ 0.78**	**$ 0.99**	**$ 2.24**
Technical				
Technical Manager (incl travel, documentation, and training)	$ 1.60	$ 2.70	$ 2.60	$ 6.90
Test and Evaluations: TD, LUA, and MUA	$ 1.20	$ 1.00	$ 1.20	$ 3.40
Sofware & Hardware Integration, Configuration	$ 2.40	$ 1.10	$ 1.10	$ 4.60
INTEGRITY PC + PCS SABI Certification	$ 2.80	$ 2.30	$ 0.90	$ 6.00
INTEGRITY PC Robustness Certification	$ 2.20	$ 1.70	$ 0.80	$ 4.70
PCS Robustness Certification	$ 1.20	$ 1.20	$ 0.40	$ 2.80
PCS HW Switch Robustness Certification	$ 1.60	$ 1.80	$ 0.60	$ 4.00
Technical Total	**$ 13.00**	**$ 11.80**	**$ 7.60**	**$ 32.40**
Transition				
Transition Planning	$ 0.20	$ 0.30	$ 0.70	$ 1.20
Travel	$ 0.02	$ 0.02	$ 0.03	$ 0.07
Transition Total	**$ 0.22**	**$ 0.32**	**$ 0.73**	**$ 1.27**
Grand TOTAL	**$ 13.69**	**$ 12.90**	**$ 9.32**	**$ 35.91**

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Air gap (networking) - Wikipedia, the Free Encyclopedia. Retrieved 2/3/2009 from http://en.wikipedia.org/wiki/Air_gap_(networking)

Baker, R. O. (2006). The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations. *Military Review*, (May-June) 13-32.

Business Case Analysis (BCA) [ACC]. Retrieved 2/13/2009, from https://acc.dau.mil/CommunityBrowser.aspx?id=32524

CFBLNET. (2007). *Combined Federated Battle Laboratories Network (CFBLNet) 2007 Annual Report*, CFBLNet.

Commander Joints Chiefs of Staff Instruction 6211.02C. (2008). Retrieved 3/8/2009 from http://www.dtic.mil/cjcs_directives/cdata/unlimit/6211_02.pdf

COSMOS Aims to Facilitate the Exchange of Data Among Allies. (2007, Fall 2007). *CADRC Currents*, pp. 1-5. Retrieved 2/13/2009, from http://www.cadrc.calpoly.edu/pdf/Currents_Fall_2007.pdf

The DODIIS Trusted Workstation (DTW) vs. The Trusted Multi-net™ (TMN). (2007). Retrieved 1/31/2009 from http:/trustedmultinet.com/docs/2007%20May,%20DTW%20vs%20TMN.doc

DoDIIS Trusted Workstation Version 3.2 Installed at Multiple Sites. (2006). Retrieved 1/31/2009 from http://www.wpafb.af.mil/news/story.asp?id=123033821

DTW - DoDIIS Trusted Workstation (2004). (DatasheetSun microsystems. Retrieved from http://www.sun-rays.org/lib/hardware/sunray/ds/go_DTW_cc.pdf

FY 2009 Joint Capability Technology Demonstrations Congressional Notification (2008). Congressional Notification Director, Defense Research and Engineering.

High Assurance Platform Program - NSA/CSS. (2009). Retrieved 1/30/2009 from http://www.nsa.gov/ia/programs/h_a_p/index.shtml

HP NetTop: A Technical Overview (2004). (Technical Overview Hewlett-Packard). Retrieved from http://h71028.www7.hp.com/enterprise/downloads/HP_NetTop_Whitepaper2.pdf

JEDI PMO to Manage Rollout of the DoDIIS Trusted Workstation (DTW). (2007). Retrieved from http://www.tcs-sec.com/documents/JEDICaseStudy.pdf

Meushaw, R., & Simard, D. (2000). NetTop Commercial Technology in High Assurance Applications. *Tech Trend Notes Preview of Tomorrow's Information Technologies*, 9(4), 1-8. Retrieved from http://www.vmware.com/pdf/TechTrendNotes.pdf

MIL-HDBK-881a dtd 30 july 2005 [ACC]. Retrieved 2/23/2009 from https://acc.dau.mil/CommunityBrowser.aspx?id=54787&lang=en-US

Network Infrastructure Reduction Concept of Operations (CONOPS) (2008). No. 1.0. MacDill AFB, Tampa, FL: USCENTCOM.

Referentia Systems Inc. (2007). *Design Description for the Agile Coalition Environment A Component of the Commander Third Fleet Command and Control (C2) Network* (Design Description No. 1.2). Honolulu, HI: Referntia Systems Inc.

Rutherford, S. (2008). *Creating the Ability to Access Information* (Brief). MacDill AFB, Tampa, FL: USSOCOM.

SELinux Symposium Case Study: US Coast Guard NetTop2 -Thin Client Implementation(2007). (BriefTrusted Computer Solutions. Retrieved from http://selinux-symposium.org/2007/slides/08-tcs.pdf

Staneszewski, D. L. (2008). *USCENTCOM OB1 Briefing*. MacDill AFB, Tampa, FL: USCENTCOM.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Jerry Gelling
   SAIC
   Tampa, Florida